۱– مبانی شبکه های بی سیم

۱-۱تشریح مقدماتی شبکه های بی سیم و کابلی

۱-۲مبانی شبکه های بیسیم

۱-۳انواع شبکه های بی سیم

۱-٤شبکه‌های بی‌سیم، کاربردها، مزایا و ابعاد

۱-٥روش های ارتباطی بی سیم

۱-٦عناصر فعال شبکه‌های محلی بی‌سیم

مقدمه

نیاز روز افزون به پویایی کارها ، استفاده از تجهیزاتی مانند تلفن همراه ، پیجرها و ... بواسطه وجود شبکه های بی سیم امکان پذیر شده است.

اگر کاربر یا شرکت یا برنامه کاربردی خواهان آن باشد که داده و اطلاعات مورد نیاز خود را به صورت متحرک در هر لحظه در اختیار داشته باشند شبکه های بی سیم جواب مناسبی برای آنها ست.

تشریح مقدماتی شبکه های بی سیم و کابلی

شبکه های محلی (LAN) برای خانه و محیط کار می توانند به دو صورت کابلی (Wired) یا بی سیم (Wireless) طراحی گردند . درابتدا این شبکه ها به روش کابلی با استفاده از تکنولوژی Ethernet طراحی می شدند اما اکنون با روند رو به افزایش استفاده از شبکه های بی سیم با تکنولوژی Wi-Fi مواجه هستیم .

در شبکه های کابلی (که در حال حاضر بیشتر با توپولوژی ستاره ای بکار می روند) بایستی از محل هر ایستگاه کاری تا دستگاه توزیع کننده (هاب یا سوئیچ) به صورت مستقل کابل کشی صورت پذیرد(طول کابل ازنوع CAT۵ نبایستی ۱۰۰ متر بیشتر باشد در غیر اینصورت از فیبر نوری استفاده میگردد) که تجهیزات بکار رفته از دونوع غیر فعال (Passive) مانند کابل ، پریز، داکت ، پچ پنل و..... . و فعال (Active)مانند هاب ،سوئیچ ،روتر ، کارت شبکه و..... هستند .

موسسه مهندسی IEEE استانداردهای ۸۰۲,۳u را برای Fast Ethernet و ۸۰۲,۳ab و۸۰۲,۳z را برای Gigabit Ethernet (مربوط به کابلهای الکتریکی و نوری) در نظر گرفته است.

شبکه های بی سیم نیز شامل دستگاه مرکزی (Access Point) می باشد که هر ایستگاه کاری می تواند حداکثر تا فاصله ۳۰ متر ی آن (بدون مانع) قرار گیرد. شبکه های بی سیم (Wlan) یکی از سه استاندارد ارتباطی Wi-Fi زیر را بکار می برند:

- ۸۰۲,۱۱b که اولین استانداردی است که به صورت گسترده بکار رفته است .
- ۸۰۲,۱۱a سریعتر اما گرانتر از ۸۰۲,۱۱b می باشد.
- ۸۰۲,۱۱g جدیدترین استاندارد که شامل هر دو استاندارد قبلی بوده و از همه گرانتر میباشد.

هر دونوع شبکه های کابلی و بی سیم ادعای برتری بر دیگری را دارند اما انتخاب صحیح با در نظر گرفتن قابلیتهای آنها میسر می باشد.

عوامل مقایسه

در مقایسه شبکه های بی سیم و کابلی می تواند قابلیتهای زیر مورد بررسی قرار گیرد:

- نصب و راه اندازی
- هزینه
- قابلیت اطمینان
- کارائی
- امنیت

نصب و راه اندازی

در شبکه های کابلی بدلیل آنکه به هر یک از ایستگاههای کاری بایستی از محل سویئچ مربوطه کابل کشیده شود با مسائلی همچون سوارخکاری ، داکت کشی ، نصب پریز و..... مواجه هستیم در ضمن اگر محل فیزیکی ایستگاه مورد نظر تغییر یابد بایستی که کابل کشی مجدد و .....صورت پذیرد

شبکه های بی سیم از امواج استفاده نموده و قابلیت تحرک بالائی را دارا هستند بنابراین تغییرات در محل فیزیکی ایستگاههای کاری به راحتی امکان پذیر می باشد برای راه اندازی آن کافیست که از روشهای زیر بهره برد:

- Ad hoc که ارتباط مستقیم یا همتا به همتا (peer to peer) تجهیزات را با یکدیگر میسر می سازد.
- Infrastructure که باعث ارتباط تمامی تجهیزات با دستگاه مرکزی می شود.

بنابراین میتوان دریافت که نصب و را ه اندازی شبکه های کابلی یا تغییرات در آن بسیار مشکلتر نسبت به مورد مشابه یعنی شبکه های بی سیم است .

هزینه

تجهیزاتی همچون هاب ، سوئیچ یا کابل شبکه نسبت به مورد های مشابه در شبکه های بی سیم ارزانتر می باشد اما درنظر گرفتن هزینه های نصب و تغییرات احتمالی محیطی نیز قابل توجه است .

قابل به ذکر است که با رشد روز افزون شبکه های بی سیم ، قیمت آن نیز در حال کاهش است .

قابلیت اطمینان

تجهیزات کابلی بسیار قابل اعتماد میباشند که دلیل سرمایه گذاری سازندگان از حدود بیست سال گذشته نیز همین می باشد فقط بایستی در موقع نصب و یا جابجائی ، اتصالات با دقت کنترل شوند.

تجهیزات بی سیم همچون Broadband Router ها مشکلاتی مانند قطع شدن‌های پیاپی، تداخل امواج الکترومغناطیس، تداخل با شبکه‌های بی‌سیم مجاور و ... را داشته اند که روند رو به تکامل آن نسبت به گذشته(مانند ۸۰۲,۱۱g) باعث بهبود در قابلیت اطمینان نیز داشته است .

کارائی

شبکه های کابلی دارای بالاترین کارائی هستند در ابتدا پهنای باند ۱۰ Mbps سپس به پهنای باندهای بالاتر(۱۰۰ Mbps و ۱۰۰۰Mbps) افزایش یافتند حتی در حال حاضر سوئیچهائی با پهنای باند ۱Gbps نیز ارائه شده است .

شبکه های بی سیم با استاندارد ۸۰۲,۱۱b حداکثر پهنای باند ۱۱Mbps و با ۸۰۲,۱۱a و ۸۰۲,۱۱g پهنای باند ٥٤ Mbps را پشتیبانی می کنند حتی در تکنولوژیهای جدید این روند با قیمتی نسبتا بالاتر به ۱۰۸Mbps نیز افزایش داده شده است علاوه بر این کارائی Wi-Fi نسبت به فاصله حساس می باشد یعنی حداکثر کارائی با افزایش فاصله نسبت به Access Point پایین خواهد آمد. این پهنای باند برای به اشتراک گذاشتن اینترنت یا فایلها کافی بوده اما برای برنامه هائی که نیاز به رد و بدل اطلاعات زیاد بین سرور و ایستگاهای کاری (Client to Server) دارند کافی نیست .

امنیت

بدلیل اینکه در شبکه های کابلی که به اینترنت هم متصل هستند، وجود دیواره آتش از الزامات است و تجهیزاتی مانند هاب یا سوئیچ به تنهایی قادر به انجام وظایف دیواره آتش نمیباشند، بایستی در چنین شبکه هایی دیواره آتش مجزایی نصب شود.

تجهیزات شبکه های بی سیم مانند Broadband Routerها دیواره آتش بصورت نرم افزاری وجود داشته و تنها بایستی تنظیمات لازم صورت پذیرد. از سوی دیگر به دلیل اینکه در شبکه‌های بی‌سیم از هوا بعنوان رسانه انتقال استفاده میشود، بدون پیاده سازی تکنیک‌های خاصی مانند رمزنگاری، امنیت اطلاعات بطور کامل تامین نمی

گردد استفاده از رمزنگاری WEP (Wired Equivalent Privacy) باعث بالا رفتن امنیت در این تجهیزات گردیده است .

جدول مقایسه ای :

نوع سرویس	شبکه های کابلی	شبکه های بی‌سیم
نصب و راه اندازی	نسبتا مشکل	آسان
هزینه	کمتر	بیشتر
قابلیت اطمینان	بالا	متوسط
کارائی	خیلی خوب	خوب
امنیت	خوب	نسبتا خوب
پویایی حرکت	محدود	پویاتر

مبانی شبکه های بیسیم

شبکه های بی سیم (Wireless) یکی از تکنولوژی های جذابی هستند که توانسته انـد توجـه بـسیاری را بـسوی خود جلب نمایند و عده ای را نیز مسحور خود نموده اند.

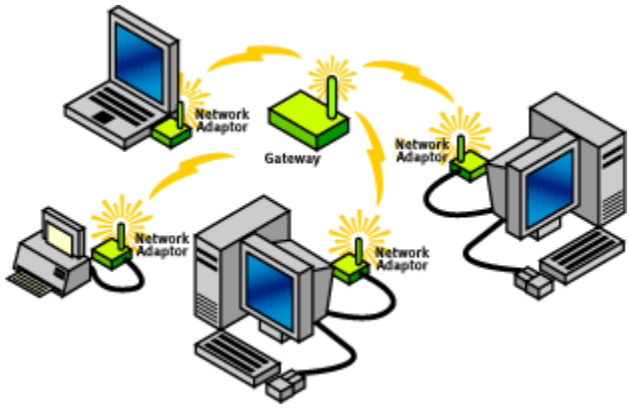
ارائه سرویس بدون سیم اینترنت یا WiFi، که امروزه در بسیاری نقاط دنیا به منظـور جـذب مـشتری و بـه عنـوان خدمتی نوین در جهت ارتقای سازمان در بازار رقابت، انجام می‌گیرد. خدمات اینترنت بی‌سیم علاوه بر مکـان‌هـای متعدد مانند هتل‌ها، نمایشگاه‌ها، بنادر، سالن‌های همایش و فرودگاه‌ها در منازل و محل‌های کار نیز عرضه می‌گـردد و موجبات رضایت خاطر مشتریان و مسافران، بـه‌خـصوص مـشتریان و مـسافران خـارجی را فـراهم آورده اسـت. بر اساس آمار تعداد کاربران این سرویس از ۱۲ میلیون نفر در سال ۲۰۰۲ به حدود ۷۰۰ میلیون نفـر در سـال ۲۰۰۸

برآورد می‌گردد. از طرفی META Group و In-Stat/MDR تخمین می‌زنند که در ۹۹٪از تولیدات شرکت‌های تولید کنندهٔ کامپیوترهای laptop که در سال ۲۰۰۷ به فروش خواهند رسید، قابلیت استفادهٔ بی‌سیم (WiFi) بطور پیش‌فرض لحاظ خواهد گردید. اینترنت بی‌سیم که تحت نام WiFi نیز شناخته می‌شود، یک تکنولوژی شبکه پرسرعت است که بطور وسیعی در خانه‌ها، مدارس، کافه‌ها، هتل‌ها و سایر مکان‌های عمومی مانند کنگره‌ها و فرودگاه‌ها مورد استفاده قرار می‌گیرد. WiFi امکان دسترسی به اینترنت، بدون نیاز به کابل یا سیم را برای وسایلی مانند کامپیوترهای کیفی (Laptop) ، کامپیوترهای جیبی (PDA) و کامپیوترهای شخصی (PC) دارای کارت Wireless فراهم می‌کند. بدین ترتیب مسافر بدون آنکه مجبور به اتصال کامپیوتر خود به خط تلفن یا شبکهٔ اتاق خود باشد، می‌تواند در محل هتل با آسودگی از اینترنت استفاده نماید.

امروزه، حدود ۵۰٪ از لپ تاپهای جدید با توانایی کارکردن بصورت بی سیم به بازار ارائه میشوند. تمام محصولات جدید لپ تاپهای اپل (Apple) هم با امکانات بی سیم و هم بلوتوث ساخته شده در درونشان به بازار عرضه میشوند. بسیاری از لپ تاپهای با سیستم عامل ویندوز مایکروسافت بطور مشابه با توانایی کار کردن بصورت بی سیم میباشند.

انواع شبکه های بی سیم

(WLANS)Wireless Local Area Networks



این نوع شبکه برای کاربران محلی از جمله محیطهای(Campus) دانشگاهی یا آزمایشگاهها که نیاز به استفاده از اینترنت دارند مفید می باشد. در این حالت اگر تعداد کاربران محدود باشند می توان بدون استفاده از Access Point این ارتباط را برقرار نمود .در غیر اینصورت استفاده از Access Point ضروری است.می توان با استفاده از آنتن های مناسب مسافت ارتباطی کاربران را به شرط عدم وجود مانع تاحدی طولانی تر نمود.

(WPANS)Wireless Personal Area Networks

دو تکنولوژی مورد استفاده برای این شبکه ها عبـارت از :IR (Infra Red) و Bluetooth (IEEE ۸۰۲,۱۵) می باشد که مجوز ارتباط در محیطی حدود ۹۰ متر را می دهد البته در IR نیاز به ارتباط مستقیم بوده و محـدودیت مسافت وجود دارد .

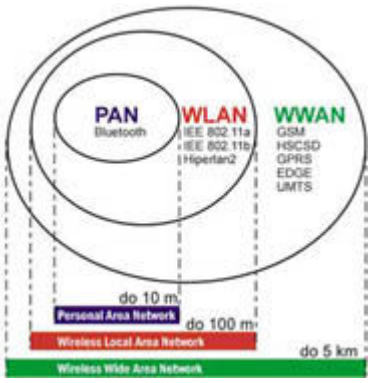
(WMANS)Wireless Metropolitan Area Networks

توسط این تکنولوژی ارتباط بین چندین شبکه یا ساختمان در یک شهر برقرار می شود برای Backup آن می توان از خطوط اجاره ای ،فیبر نوری یا کابلهای مسی استفاده نمود .

(WWANS)Wireless Wide Area Networks

برای شبکه هائی با فواصل زیاد همچون بین شهرها یا کشورها بکار می رود این ارتباط از طریق آنتن ها ی بی سیم یا ماهواره صورت می پذیرد .

جدول و شکل زیر کاربرد انواع شبکه های بی سیم در فواصل متفاوت را نشان می دهد:



Meters	Network
۰-۱۰	Personal Area Network
۰-۱۰۰	Local Area Network
۰-۱۰۰۰۰	Wide Area Network

شبکه‌های بی‌سیم، کاربردها، مزایا و ابعاد

تکنولوژی شبکه‌های بی‌سیم، با استفاده از انتقال داده‌ها توسط اموج رادیویی، در ساده‌ترین صورت، به تجهیزات سخت‌افزاری امکان می‌دهد تا بدون‌استفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه‌های بی‌سیم بازه‌ی وسیعی از کاربردها، از ساختارهای پیچیده‌یی چون شبکه‌های بی‌سیم سلولی -که اغلب برای تلفن‌های همراه استفاده می‌شود- و شبکه‌های محلی بی‌سیم (WLAN – Wireless LAN) گرفته تا انوع ساده‌یی چون هدفون‌های بی‌سیم، را شامل می‌شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده می‌کنند، مانند صفحه کلیدها، ماوس‌ها و برخی از گوشی‌های همراه، در این دسته‌بندی جای می‌گیرند. طبیعی‌ترین مزیت استفاده از این شبکه‌ها عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل به این‌گونه شبکه‌ها و هم‌چنین امکان ایجاد تغییر در ساختار مجازی آن‌هاست. از نظر ابعاد ساختاری، شبکه‌های بی‌سیم به سه دسته تقسیم می‌گردند : WWAN، WLAN و WPAN.

مقصود از WWAN، که مخفف Wireless WAN است، شبکه‌هایی با پوشش بی‌سیم بالاست. نمونه‌یی از این شبکه‌ها، ساختار بی‌سیم سلولی مورد استفاده در شبکه‌های تلفن همراه است. WLAN پوششی محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می‌کند. کاربرد شبکه‌های WPAN یا Wireless Personal Area Network برای موارد خانه‌گی است. ارتباطاتی چون Bluetooth و مادون قرمز در این دسته قرار می‌گیرند.

شبکه‌های WPAN از سوی دیگر در دسته‌ی شبکه‌های Ad Hoc نیز قرار می‌گیرند. در شبکه‌های Ad hoc، یک سخت‌افزار، به‌محض ورود به فضای تحت پوشش آن، به‌صورت پویا به شبکه اضافه می‌شود. مثالی از این نوع شبکه‌ها، Bluetooth است. در این نوع، تجهیزات مختلفی از جمله صفحه کلید، ماوس، چاپگر، کامپیوتر کیفی یا جیبی و حتی گوشی تلفن همراه، در صورت قرارگرفتن در محیط تحت پوشش، وارد شبکه شده و امکان رد و بدل داده‌ها با دیگر تجهیزات متصل به شبکه را می‌یابند. تفاوت میان شبکه‌های Ad hoc با شبکه‌های محلی بی‌سیم (WLAN) در ساختار مجازی آن‌هاست. به‌عبارت دیگر، ساختار مجازی شبکه‌های محلی بی‌سیم بر پایه‌ی طرحی ایستاست درحالی‌که شبکه‌های Ad hoc از هر نظر پویا هستند. طبیعی‌ست که در کنار مزایایی که این پویایی برای استفاده کننده‌گان فراهم می‌کند، حفظ امنیت چنین شبکه‌هایی نیز با مشکلات بسیاری همراه است. با این وجود،

عملاً یکی از راه حل‌های موجود برای افزایش امنیت در این شبکه‌ها، خصوصاً در انـواعی همچـون Bluetooth، کاستن از شعاع پوشش سیگنال‌های شبکه است. در واقع مستقل از این حقیقت که عمل‌کرد Bluetooth بر اساس فرستنده و گیرنده‌های کم‌توان استوار است و این مزیت در کامپیوترهـای جیبـی برتـری قابـل‌توجـه‌یـی محـسوب می‌گردد، همین کمی توان سخت‌افزار مربوطه، موجب وجود منطقه‌ی محدود تحت پوشـش اسـت کـه در بررسـی امنیتی نیز مزیت محسوب می‌گردد. به‌عبارت دیگر این مزیت به‌همراه استفاده از کدهای رمز نه‌چندان پیچیـده، تنهـا حربه‌های امنیتی این دسته از شبکه‌ها به‌حساب می‌آیند.

روش های ارتباطی بی سیم :

تجهیزات و شبکه های کامپیوتری بی سیم بر دو قسم Indoor یا درون سازمانی و Outdoor یا بـرون سـازمانی تولید شده و مورد استفاده قرار می گیرند.

شبکه های بی سیم Indoor :

نیاز سازمان ها و شرکت ها برای داشتن شبکه ای مطمئن و وجود محدودیت در کابل کشی ، متخصصین را تشویق به پیدا کردن جایگزین برای شبکه کامپیوتری کرده است. شبکه های Indoor به شبکه هایی اتلاق می شود که در داخل ساختمان ایجاد شده باشد. این شبکه ها بر دو گونه طراحی می شوند. شبکه های Ad hoc و شـبکه هـای Infra Structure. در شبکه های Ad hoc دستگاه متمرکز کننده مرکزی وجـود نـدارد و کامپیوترهـای دارای کارت شبکه بی سیم هستند. استراتژی Ad hoc برای شبکه های کوچک بـا تعـداد ایـستگاه کـاری محـدود قابـل استفاده است. روش و استراتژی دوم جهت پیاده سازی استاندارد شبکه بی سیم ، شـبکه Infra Structure مـی باشد. در این روش یک یا چند دستگاه متمرکز کننده به نام Access Point مسؤولیت برقراری ارتباط را برعهده دارد.

شبکه های بی سیم Outdoor :

برقراری ارتباط بی سیم در خارج ساختمان به شبکه بی سیم Outdoor شـهرت دارد. در ایـن روش داشـتن دیـد مستقیم یا Line Of Sight ، ارتفاء دو نقطه و فاصله، معیارهایی بـرای انتخـاب نـوع Access Point و آنـتن هستند.

انواع ارتباط :

شبکه بی سیم Outdoor با سه توپولوژی Point To Point ، Point To Multipoint و Mesh قابل پیاده سازی می باشد.

Point To point :

در این روش ارتباط دو نقطه مدنظر می باشد. در هر یک از قسمت ها آنتن و AccessPoint نصب شده و ارتباط این دو قسمت برقرار می شود.

Point To Multi Point :

در این روش یک نقطه به عنوان مرکز شبکه درنظر گرفته می شود و سایر نقاط به این نقطه در ارتباط هستند.

Mesh :

ارتباط بی سیم چندین نقطه بصورت های مختلف را توپولوژی Mesh می گویند. در این روش ممکن است چندین نقطه مرکزی وجود داشته باشد که با یکدیگر در ارتباط هستند.

ارتباط بی سیم بین دو نقطه به عوامل زیر بستگی دارد :

۱- توان خروجی Access Point (ارسال اطلاعات)

۲- میزان حساسیت Access Point(دریافت اطلاعات)

۳- توان آنتن

۱–توان خروجی Access Point :

یکی از مشخصه های طراحی سیستم های ارتباطی بی سیم توان خروجی Access Point می باشد. هرچقدر این توان بیشتر باشد قدرت سیگنال های توایدی و برد آن افزایش می یابد.

۲–میزان حساسیت Access Point :

از مشخصه های تعیین کننده در کیفیت دریافت امواج تولید شده توسط Access Point نقطه مقابل میزان حساسیت Access Point می باشد. هرچقدر این حساسیت افزایش یابد احتمال عدم دریافت سیگنال کمتر می باشد و آن تضمین کننده ارتباط مطمئن و مؤثر خواهد بود.

۳–توان آنتن :

در مورد هر آنتن توان خروجی آنتن و زاویه پوشش یا انتشار مشخصه های حائز اهمیت مـی باشـند در ایـن راسـتا آنتن های مختلفی با مشخصه های مختلف تـوان و زاویـه انتـشار بوجـود آمـده اسـت کـه آنـتن هـای Omni ، Sectoral ، Parabolic ، Panel ، Solied و . . . . مثال هایی از آن هستند

عناصر فعال شبکه‌های محلی بی‌سیم

در شبکه‌های محلی بی‌سیم معمولاً دو نوع عنصر فعال وجود دارد :

–ایستگاه بی سیم

ایستگاه یا مخدوم بی‌سیم به طور معمول یک کامپیوتر کیفی یا یک ایستگاه کاری ثابت است که توسط یـک کـارت شبکه‌ی بی‌سیم به شبکه‌ی محلی متصل می‌شود. این ایستگاه می‌تواند از سوی دیگر یک کامپیوتر جیبی یا حتی یـک پویش گر بارکد نیز باشد. در برخی از کاربردها برای این‌که استفاده از سیم در پایانه‌هـای رایانـه‌یـی بـرای طـراح و مجری دردسرساز است، برای این پایانه‌ها که معمولاً در داخل کیوسک‌هایی به‌همین منظور تعبیه می‌شـود، از امکـان اتصال بی‌سیم به شبکه‌ی محلی استفاده می‌کنند. در حال حاضر اکثر کامپیوترهای کیفی موجود در بازار به این امکان به‌صورت سرخود مجهز هستند و نیازی به اضافه‌کردن یک کارت شبکه‌ی بی‌سیم نیست.

کارت‌های شبکه‌ی بی‌سیم عموماً برای استفاده در چاک‌های PCMCIA است. در صورت نیـاز بـه اسـتفاده از ایـن کارت‌ها برای کامپیوترهای رومیزی و شخصی، با استفاده از رابطی این کارت‌ها را بر روی چاک‌های گسترش PCI نصب می‌کنند.

– نقطه ی دسترسی

نقاط دسترسی در شبکه‌های بی‌سیم، همان‌گونه که در قسمت‌های پیش نیز در مورد آن صحبت شد، سخت افزارهای فعالی هستند که عملاً نقش سوییچ در شبکه‌های بی‌سیم را بازی‌کرده، امکان اتصال به شبکه های سیمی را نیز دارند. در عمل ساختار بستر اصلی شبکه عموماً سیمی است و توسط این نقاط دسترسی، مخدوم‌ها و ایستگاه‌های بـی‌سـیم به شبکه‌ی سیمی اصلی متصل می‌گردد.

برد و سطح پوشش

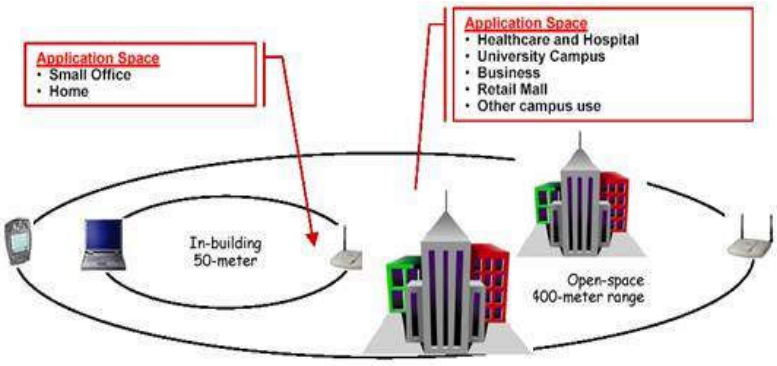
شعاع پوشش شبکه‌ی بی‌سیم بر اساس استاندارد ۸۰۲,۱۱ به فاکتورهای بسیاری بستگی دارد که برخی از آن‌ها به شرح زیر هستند :

- پهنای باند مورد استفاده
- منابع امواج ارسالی و محل قرارگیری فرستنده‌ها و گیرنده‌ها
- مشخصات فضای قرارگیری و نصب تجهیزات شبکه‌ی بی‌سیم
- قدرت امواج
- نوع و مدل آنتن

شعاع پوشش از نظر تئوری بین ۲۹متر (برای فضاهای بسته‌ی داخلی) و ٤٨٥متر (برای فضاهای باز) در استاندارد ۸۰۲,۱۱b متغیر است. با این‌وجود این مقادیر، مقادیری متوسط هستند و در حال حاضر با توجه به گیرنده‌ها و فرستنده‌های نسبتاً قدرت‌مندی که مورد استفاده قرار می‌گیرند، امکان استفاده از این پروتکل و گیرنده‌ها و فرستنده‌های آن، تا چند کیلومتر هم وجود دارد که نمونه‌های عملی آن فراوان‌اند.

با این وجود شعاع کلی‌یی که برای استفاده از این پروتکل (۸۰۲,۱۱b) ذکر می‌شود چیزی میان ۵۰ تا ۱۰۰متر است. این شعاع عمل‌کرد مقداری‌ست که برای محل‌های بسته و ساختمان‌های چند طبقه نیز معتبر بوده و می‌تواند مورد استناد قرار گیرد.

شکل زیر مقایسه‌یی میان بردهای نمونه در کاربردهای مختلف شبکه‌های بی‌سیم مبتنی بر پروتکل ۸۰۲,۱۱b را نشان می‌دهد :

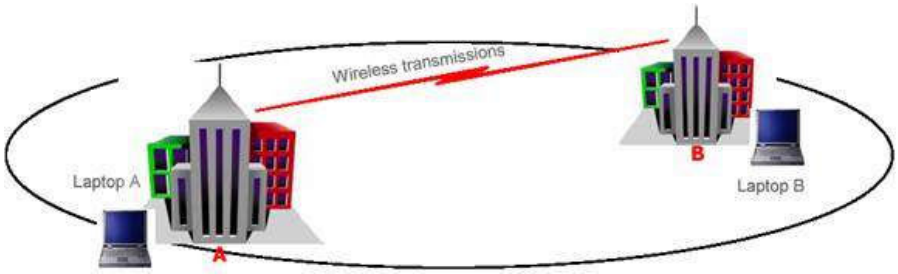


یکی از عمل‌کردهای نقاط دسترسی به عنوان سوییچ‌های بی‌سیم، عمل اتصال میان حوزه‌های بی‌سیم است. به‌عبارت دیگر با استفاده از چند سوییچ بی‌سیم می‌توان عمل‌کردی مشابه Bridge برای شبکه‌های بی‌سیم را به‌دست آورد.

اتصال میان نقاط دست‌رسی می‌تواند به صورت نقطه‌به‌نقطه، برای ایجاد اتصال میان دو زیرشبکه به یکدیگر، یا به صورت نقطه‌یی به چند نقطه یا بالعکس برای ایجاد اتصال میان زیرشبکه‌های مختلف به یکدیگر به‌صورت همزمان صورت گیرد.

نقاط دسترسی‌یی که به عنوان پل ارتباطی میان شبکه‌های محلی با یکدیگر استفاده می‌شوند از قدرت بالاتری برای ارسال داده استفاده می‌کنند و این به‌معنای شعاع پوشش بالاتر است. این سخت‌افزارها معمولاً برای ایجاد اتصال میان نقاط و ساختمان‌هایی به‌کار می‌روند که فاصله‌ی آن‌ها از یکدیگر بین ۱ تا ۵ کیلومتر است. البته باید توجه داشت که این فاصله، فاصله‌یی متوسط بر اساس پروتکل ۸۰۲,۱۱b است. برای پروتکل‌های دیگری چون ۸۰۲,۱۱a می‌توان فواصل بیشتری را نیز به‌دست آورد.

شکل زیر نمونه‌یی از ارتباط نقطه به نقطه با استفاده از نقاط دست‌رسی مناسب را نشان می‌دهد :



از دیگر استفاده‌های نقاط دسترسی با برد بالا می‌توان به امکان توسعه‌ی شعاع پوشش شبکه های بی‌سیم اشاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوشش یک شبکه‌ی بی‌سیم، می‌توان از چند نقطه‌ی دست‌رسی بی‌سیم به‌صورت همزمان و پشت به پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا می‌توان با استفاده از یک فرستنده‌ی دیگر در بالای هریک از ساختمان‌ها، سطح پوشش شبکه را تا ساختمان‌های دیگر گسترش داد.

WIFI-۲

۲-۱ Wifiچیست؟

۲-۲چرا WiFi را بکار گیریم؟

۲-۳معماری

۲-٤شبکه های اطلاعاتی

۲-٥Wifi چگونه کار می کند؟

۲-٦IEEE ۸۰۲/۱۱

۲-۷کاربرد های wifi

۲-۸دلایل رشد wifi

۲-۹نقاط ضغف wifi

مقدمه

شبکه های بیسیم از دیر باز از امواخ رادیویی برای انتقال سیگنالها سود می بردند در این قبیل از شبکه ها یک قطعه سخت افزاری اطلاعات را به امواج رادیویی تبدیل میکند و سپس ان ها را از طریق انتن های موجود در شبکه ارسال می کند اما در طرف دیگر یک دریافت کنند ه بدون سیم مستقر است تا با دریافت سیگنال های ارسالی و تبدیل آنها به اطلاعات و رمزگشایی اطلاعات آنها را به داده های قابل فهم برای رایانه تبدیل کند .یکی از راههای ارسال داده ها در سیتم های بیسیم استفاده از تکنولوژی wifi می باشد که به تازگی در شبکه ها به وجود آمده است و مراحل پیشرفت خود را به تازگی آغاز نموده است.

Wifiچیست؟

wi-fi که مخفف عبارت wireless fidelity است، یک تکنولوژی ارتباطات بی سیم یا همون wireless می باشد که مزایای بسیار و معایب کمی دارد. شبکه‌های محلی بی‌سیم WLAN که تحت پوشش مجوعه استانداردهای ۸۰۲,۱۱ IEEE فعال میباشند را Wi-Fi مینامند.

اما در حقیقت طیف گسترده تری از استانداردهای WLAN محسوب می شود که شامل ۸۰۲,۱۱a و ظهور سریع استاندارد ۸۰۲,۱۱g میشود . این استاندارد توسط اتحادیه سازگاری اترنت بی سیم (WECA) به ثبت رسیده است .وای فای تا حدود ۱۰۰ فوت (۳۰/۵ متر) تمام جهت ها را تحت پوشش قرار می دهد هر چند دیوارها و منابع ممکن است این محدوده را کاهش دهد .برای مکان های بزرگتر باید از تقویت کننده های سیگنال برای افزایش این محدوده استفاده کرد. مهمترین مزیت وای فای سادگی آن است. در این مدل حداکثر سرعت انتقال اطلاعات ۱۱ Mbpsاست و از فرکانس رادیویی ٤/۲ گیگاهرتز استفاده می کند. برای سرعت بخشیدن به این استاندارد مدل دیگری نیز به نام ۸۰۲,۱۱b+ ایجاد شده که سرعت انتقال را تا ۲۲mbps افزایش می دهد. در مدل ۸۰۲,۱۱a سرعت اطلاعات حدود ٥٤Mbps است و از فرکانس ٥GHz استفاده می شود. به طور حتم این مدل در آینده ای نه چندان دور جای ۸۰۲,۱۱b را خواهد گرفت به زبانی ساده، سیستم Wi-Fi را می توان به یک جفت واکی – تاکی که شما از آن برای مکالمه با دوستان خود استفاده می کنید تشبیه نمود. این لوازم، رادیوهای کوچک

و ساده ای هستند که قادرند تا سیگنال های رادیویی را ارسال و دریافت نمایند. هنگامی که شما بوسیله آنها صحبت می کنید، میکروفون دستگاه، صدای شما را دریافت نموده و با تلفیق آن با امواج رادیویی، از طریق آنتن آنها را ارسال می کند. در طرف دیگر، دستگاه مقصد، با دریافت سیگنال ارسال شده از طرف شما توسط آنتن، آنها را آشکار سازی نموده و از طریق بلندگوی دستگاه، صدای شما را پخش خواهد کرد. توان خروجی و یا قدرت فرستنده این گونه لوازم اغلب در حدود یک چهارم وات است و با این وصف، برد آنها چیزی در حدود ۵۰ تا ۱۰۰متر می رسد.

در تکنولوژی وای فای این امکان فراهم شده که طیف رادیویی موجود را بتوان بین تعداد زیادی و متنوعی از گیرنده ها و فرستنده ها توزیع کرد و همه آن ها نیز قابلیت در یافت سیگنال ارسالی را داشته باشند.

چرا WiFi را بکار گیریم؟

نیروی کاری امروزه که با دستیارهای شخصی دیجیتالی (PDA ها)، لپ تاپ ها و دیگر وسایل متحرک (موبایل) تجهیز شده اند، تقاضای دسترسی به شبکهء شما را از هر کجا که باشند، بدون دردسر یک شبکه ثابت، می نمایند . WiFiبه کار و تجارت شما اجازه میدهد که یک شبکه را سریعتر و با هزینه پایین تر و با انعطاف پذیری بیشتر نسبت به سیستم با سیم ، بکار گیرید . سودمندی WiFi نیز افزایش می یابد، از آنجائیکه کارمندان می توانند مدت زیادتری به یک شبکه متصل بوده، و قادر خواهند بود که با همکارانشان در زمان و مکانی که نیاز باشد کار نمایند .

شبکه های WiFi نسبت به شبکه های باسیم روان تر میباشند. یک شبکه دیگر بیش از این یک چیز ثابت نمی باشد، شبکه ها می توانند در یک بعداظهر ایجاد یا از هم باز شوند بجای اینکه روزها یا هفته ها نیاز به ایجاد یک شبکهء کابلی ساختار یافته باشد . این شبکه‌ها می‌توانند دارای کابردهای خانگی، اداری یا صنعتی باشند که نمونه‌هایی از آنها را می‌توان به شرح زیر نام برد:

۱.- شبکه‌های توزیع اینترنت در مکان های عمومی مانند فرودگاه ها ،مراکز تجاری و ... (Hot Spot)

۲- شبکه‌های محلی بی‌سیم در شرکت‌ها و ادارات با هدف انتقال اطلاعات (Data)

۳- شبکه‌های محلی بی‌سیم با هدف انتقال مکالمات صدا (VOIP)

٤-شبکه‌های محلی بی‌سیم با هدف انتقال تصویر (CCTV , Video Conference)

٥.- شبکه‌های محلی بی‌سیم با هدف استفاده در سیستم‌های امنیتی(Security)

معماری شبکه‌های محلی بی‌سیم

معماری ۸۰۲,۱۱ از عناصر ساختمانی متعددی تشکیل شده است که در کنار هم، سـّیار بودن ایستگاه‌هـای کـاری را پنهان از دید لایه‌های فوقانی برآورده می‌سازد. ایستگاه بی‌سیم یا به اختصار ایـستگاه (STA)، بنیـادی‌تـرین عنـصر ساختمانی در یک شبکه محلی بی‌سیم است. یک ایستگاه، دستگاهی است که بـر اسـاس تعـاریف و پروتکـل‌هـای ۸۰۲,۱۱ (لایه‌های MAC و PHY) عمل کرده و به رسانه بی‌سیم متصل اسـت. توجـه داشـته باشـید کـه براسـاس تعریف کلاسیکِ شبکه‌های کامپیوتری، یک شبکه کامپیوتری مجموعه‌ای از کامپیوترهای **مستقل** و **متصل** اسـت کـه منظور از اتصال در این تعریف، توانایی جابجایی و مبادله پیام‌ها است. ایستگاه‌های کاری بی‌سیم امروزی عمدتاً بـه صورت مجموعه سخت‌افزاری/نرم‌افزاری کارت‌های شبکه بی‌سیم پیـاده‌سـازی مـی‌شـوند. همچنـین یـک ایـستگاه می‌تواند یک کامپیوتر قابل حمل، کامپیوتر کفدستی و یا یک نقطه دسترسی باشد. نقطه دسترسی در واقـع در حکـم پلی است که ارتباط ایستگاه‌های بی‌سیم را با سیستم توزیع یا شـبکه سـیمی برقـرار مـی‌سـازد. کـوچکترین عنـصر ساختمانی شبکه‌های محلی بی‌سیم در استاندارد ۸۰۲,۱۱ *مجموعه سرویس پایه* یا BSS نامیـده مـی‌شـود. در واقـع BSS مجموعه‌ای از ایستگاه‌های بی‌سیم است.

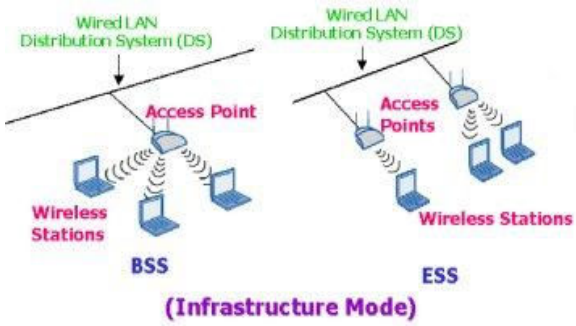
همبندی‌های ۸۰۲.۱۱

در یک تقسیم بندی کلی می‌توان دو همبندی را برای شبکه‌های محلی بی‌سیم در نظر گرفت. سـاده‌تـرین همبنـدی، **فی‌البداهه** (Ad Hoc) و براساس فرهنگ واژگان استاندارد ۸۰۲,۱۱، IBSS است. در این همبنـدی ایـستگاه‌هـا از طریق رسانه بی‌سیم به صورت نظیر به نظیر با یکدیگر در ارتباط هستند و برای تبادل داده (تبادل پیام) از تجهیـزات یا ایستگاه واسطی استفاده نمی‌کنند. واضح است که در این همبندی به سبب محدودیت‌های فاصـله هـر ایـستگاهی ضرورتاً نمی‌تواند با تمام ایستگاه‌های دیگر در تماس باشد. به این ترتیب شرط اتصال مـستقیم در همبنـدی IBSS

آن است که ایستگاه‌ها در محدوده عملیاتی بی‌سیم یا همان بُرد شبکه بی‌سیم قرار داشته باشند. شکل ۲-۱ همبنـدی IBSSرا نشان می‌دهد.

شکل ۲-۱- همبندی فی‌البداهه یا IBSS

همبندی دیگر زیرساختار است. در این همبندی عنصر خاصی موسوم به نقطه دسترسی وجود دارد. نقطه دسترسـی ایستگاه‌های موجود در یک مجموعه سرویس را به سیستم توزیع متصل می‌کند. در این هم بندی تمام ایستگاه‌ها بـا نقطه دسترسی تماس می‌گیرند و اتصال مستقیم بین ایستگاه‌هـا وجـود نـدارد در واقـع نقطهدسترسـی وظیفـه دارد فریم‌ها (قاب‌های داده) را بین ایستگاه‌ها توزیع و پخش کند. شکل ۲-۲ همبندی زیرساختار را نشان می‌دهد.



شکل۲-۲- همبندی زیرساختار در دوگونه BSS و ESS

در این هم بندی سیستم توزیع، رسانه‌ای است که از طریق آن نقطه دسترسی (AP) با سایر نقاط دسترسی در تماس است و از طریق آن می‌تواند فریم‌ها را به سایر ایستگاه‌ها ارسال نماید. از سوی دیگر می‌تواند بسته‌هـا را در اختیـار ایستگاه‌های متصل به شبکه سیمی نیز قراردهد. در استاندارد ۸۰۲,۱۱ توصیف ویـژه‌ای بـرای سیـستم توزیـع ارائـه نشده است، لذا محدودیتی برای پیاده سازی سیستم توزیع وجود ندارد، در واقع این استاندارد تنها خدماتی را معین

می‌کند که سیستم توزیع می‌بایست ارائه نماید. بنابراین سیستم توزیع می‌تواند یک شبکه ۸۰۲,۳ معمولی و یا دستگاه خاصی باشد که سرویس توزیع مورد نظر را فراهم می‌کند.

استاندارد ۸۰۲,۱۱ با استفاده از همبندی خاصی محدوده عملیاتی شبکه را گسترش می‌دهد. این همبندی به شکل *مجموعه سرویس گسترش یافته* (ESS) بر پا می‌شود. در این روش یک مجموعه گسترده و متشکل از چندین BSS یا *مجموعه سرویس پایه* از طریق نقاط دسترسی با یکدیگر در تماس هستند و به این ترتیب ترافیک داده بین مجموعه‌های سرویس پایه مبادله شده و انتقال پیام‌ها شکل می‌گیرد. در این همبندی ایستگاه‌ها می‌توانند در محدوده عملیاتی بزرگ‌تری گردش نمایند. ارتباط بین نقاط دسترسی از طریق سیستم توزیع فراهم می‌شود. در واقع سیستم توزیع ستون فقرات شبکه‌های محلی بی‌سیم است و می‌تواند با استفاده از فنّاوری بی‌سیم یا شبکه‌های سیمی شکل گیرد. سیستم توزیع در هر نقطه دسترسی به عنوان یک لایه عملیاتی ساده است که وظیفه آن تعیین گیرنده پیام و انتقال فریم به مقصدش می‌باشد. نکته قابل توجه در این همبندی آن است که تجهیزات شبکه خارج از حوزه ESS تمام ایستگاه‌های سیّار داخل ESS را صرفنظر از پویایی و تحرکشان به صورت یک شبکه منفرد در سطح لایه MAC تلقی می‌کنند. به این ترتیب پروتکل‌های رایج شبکه‌های کامپیوتری کوچکترین تأثیری از سیّار بودن ایستگاه‌ها و رسانه بی‌سیم نمی‌پذیرند. جدول ۲-۱ همبندی‌های رایج در شبکه‌های بی‌سیم مبتنی بر ۸۰۲,۱۱ را به اختصار جمع بندی می‌کند.

۸۰۲,۱۱ **Topologies**		
Independent Basic Service Set (IBSS) ("Ad Hoc" or "Peer to Peer")	**Infrastructure**	
	Basic Service Set (BSS)	Extended Service Set (ESS)

جدول ۲-۱- همبندیهای رایج در استاندارد ۸۰۲,۱۱

خدمات ایستگاهی

بر اساس این استاندارد خدمات خاصی در ایستگاه‌های کاری پیاده‌سازی می‌شوند. در حقیقت تمام ایستگاه‌های کاری موجود در یک شبکه محلی مبتنی بر ۸۰۲,۱۱ و نیز نقاط دسترسی موظف هستند که خدمات ایستگاهی را فراهم نمایند. با توجه به اینکه امنیت فیزیکی به منظور جلوگیری از دسترسی غیر مجاز بر خلاف شبکه‌های سیمی، در شبکه‌های بی‌سیم قابل اعمال نیست استاندارد ۸۰۲,۱۱ خدمات هویت سنجی را به منظور کنترل دسترسی به شبکه تعریف می‌نماید. سرویس هویت سنجی به ایستگاه کاری امکان می‌دهد که ایستگاه دیگری را شناسایی نماید. قبل از اثبات هویت ایستگاه کاری، آن ایستگاه مجاز نیست که از شبکه بی‌سیم برای تبادل داده استفاده نماید. در یک تقسیم بندی کلی ۸۰۲,۱۱ دو گونه خدمت هویت سنجی را تعریف می‌کند:

- Open System Authentication
- Shared Key Authentication

روش اول، متد پیش فرض است و یک فرآیند دو مرحله‌ای است. در ابتدا ایستگاهی که می‌خواهد توسط ایستگاه دیگر شناسایی و هویت سنجی شود یک فریم مدیریتی هویت سنجی شامل شناسه ایستگاه فرستنده، ارسال می‌کند. ایستگاه گیرنده نیز فریمی در پاسخ می‌فرستد که آیا فرستنده را می‌شناسد یا خیر. روش دوم کمی پیچیده‌تر است و فرض می‌کند که هر ایستگاه از طریق یک کانال مستقل و امن، یک کلید مشترک سّری دریافت کرده است. ایستگاه‌های کاری با استفاده از این کلید مشترک و با بهره‌گیری از پروتکلی موسوم به WEP اقدام به هویت سنجی یکدیگر می‌نمایند. یکی دیگر از خدمات ایستگاهی خاتمه ارتباط یا خاتمه هویت سنجی است. با استفاده از این خدمت، دسترسی ایستگاهی که سابقاً مجاز به استفاده از شبکه بوده است، قطع می‌گردد.

در یک شبکه بی‌سیم، تمام ایستگاه‌های کاری و سایر تجهیزات قادر هستند ترافیک داده‌ای را "بشنوند" – در واقع ترافیک در بستر امواج مبادله می‌شود که توسط تمام ایستگاه‌های کاری قابل دریافت است. این ویژگی سطح امنیتی یک ارتباط بی‌سیم را تحت تأثیر قرار می‌دهد. به همین دلیل در استاندارد ۸۰۲,۱۱ پروتکلی موسوم به WEP تعبیه شده است که برروی تمام فریم‌های داده و برخی فریم‌های مدیریتی و هویت سنجی اعمال می‌شود. این استاندارد در پی آن است تا با استفاده از این الگوریتم سطح اختفاء وپوشش را معادل با شبکه‌های سیمی نماید.

خدمات توزیع

خدمات توزیع عملکرد لازم در همبندی‌های مبتنی بر سیستم توزیع را مهیا می‌سازد. معمولاً خدمات توزیع توسط نقطه دسترسی فراهم می‌شوند. خدمات توزیع در این استاندارد عبارتند از:

- پیوستن به شبکه- خروج از شبکه بی‌سیم- پیوستن مجدد- توزیع- مجتمع سازی

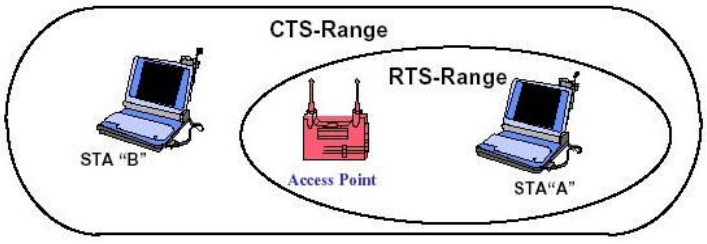
سرویس اول یک ارتباط منطقی میان ایستگاه سیّار و نقطه دسترسی فراهم می‌کند. هر ایستگاه کاری قبل از ارسال داده می‌بایست با یک نقطه دسترسی برروی سیستم میزبان مرتبط گردد. این عضویت، به سیستم توزیع امکان می‌دهد که فریم‌های ارسال شده به سمت ایستگاه سیّار را به درستی در اختیارش قرار دهد. خروج از شبکه بی‌سیم هنگامی بکار می‌رود که بخواهیم اجباراً ارتباط ایستگاه سیّار را از نقطه دسترسی قطع کنیم و یا هنگامی که ایستگاه سیّار بخواهد خاتمه نیازش به نقطه دسترسی را اعلام کند. سرویس پیوستن مجدد هنگامی مورد نیاز است که ایستگاه سیّار بخواهد با نقطه دسترسی دیگری تماس بگیرد. این سرویس مشابه "پیوستن به شبکه بی‌سیم" است با این تفاوت که در این سرویس ایستگاه سیّار نقطه دسترسی قبلی خود را به نقطه دسترسی جدیدی اعلام می‌کند که قصد دارد به آن متصل شود. پیوستن مجدد با توجه به تحرک و سیّار بودن ایستگاه کاری امری ضروری و اجتناب ناپذیر است. این اطلاع، (اعلام نقطه دسترسی قبلی) به نقطه دسترسی جدید کمک می‌کند که با نقطه دسترسی قبلی تماس گرفته و فریم‌های بافر شده احتمالی را دریافت کند که به مقصد این ایستگاه سیّار فرستاده شده‌اند. با استفاده از سرویس توزیع فریم‌های لایه MAC به مقصد مورد نظرشان می‌رسند. مجتمع سازی سرویسی است که شبکه محلی بی‌سیم را به سایر شبکه‌های محلی و یا یک یا چند شبکه محلی بی‌سیم دیگر متصل می‌کند. سرویس مجتمع سازی فریم‌های ۸۰۲,۱۱ را به فریم‌هایی ترجمه می‌کند که بتوانند در سایر شبکه‌ها (به عنوان مثال ۸۰۲,۳) جاری شوند. این عمل ترجمه دو طرفه است بدان معنی که فریم‌های سایر شبکه‌ها نیز به فریم‌های ۸۰۲,۱۱ ترجمه شده و از طریق امواج در اختیار ایستگاه‌های کاری سیّار قرار می‌گیرند.

دسترسی به رسانه

روش دسترسی به رسانه در این استاندارد CSMA/CA است که تاحدودی به روش دسترسی CSMA/CD شباهت دارد. در این روش ایستگاه‌های کاری قبل از ارسال داده کانال رادیویی را کنترل می‌کنند و در صورتی که کانال آزاد باشد اقدام به ارسال می‌کنند. در صورتی که کانال رادیویی اشغال باشد با استفاده از الگوریتم خاصی به اندازه یک زمان تصادفی صبر کرده و مجدداً اقدام به کنترل کانال رادیویی می‌کنند. در روش CSMA/CA ایستگاه فرستنده ابتدا کانال فرکانسی را کنترل کرده و در صورتی که رسانه به مدت خاصی موسوم به DIFS آزاد باشد اقدام به ارسال می‌کند. گیرنده فیلد کنترلی فریم یا همان CRC را چک می‌کند و سپس یک فریم تصدیق می‌فرستد. دریافت تصدیق به این معنی است که تصادمی بروز نکرده است. در صورتی که فرستنده این تصدیق را دریافت نکند، مجدداً فریم را ارسال می‌کند. این عمل تا زمانی ادامه می‌یابد که فریم تصدیق ارسالی از گیرنده توسط فرستنده دریافت شود یا تکرار ارسال فریم‌ها به تعداد آستان‌های مشخصی برسد که پس از آن فرستنده فریم را دور می‌اندازد.

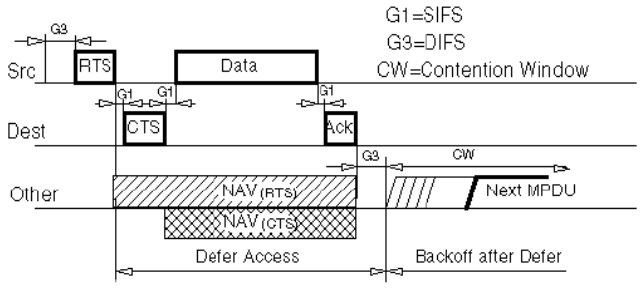
در شبکه‌های بی‌سیم بر خلاف اترنت امکان شناسایی و آشکار سازی تصادم به دو علت وجود ندارد:

۱. پیاده سازی مکانیزم آشکار سازی تصادم به روش ارسال رادیویی دوطرفه نیاز دارد که با استفاده از آن ایستگاه سیّار بتواند در حین ارسال، سیگنال را دریافت کند که این امر باعث افزایش قابل توجه هزینه می‌شود.
۲. در یک شبکه بی‌سیم، بر خلاف شبکه‌های سیمی، نمی‌توان فرض کرد که تمام ایستگاه‌های سیّار امواج یکدیگر را دریافت می‌کنند. در واقع در محیط بی‌سیم حالاتی قابل تصور است که به آنها *نقاط پنهان* می‌گوییم. در شکل زیر ایستگاه‌های کاری "A" و "B" هر دو در محدوده تحت پوشش نقطه دسترسی هستند ولی در محدوده یکدیگر قرار ندارند.



شکل ۲-۳- روزنه‌های پنهان

برای غلبه بر این مشکل، استاندارد ۸۰۲,۱۱ از تکنیکی موسوم به *اجتناب از تصادم* و مکانیزم تصدیق استفاده می‌کند. همچنین با توجه به احتمال بروز روزنه‌های پنهان و نیز به منظور کاهش احتمال تصادم در این استاندارد از روشی موسوم به *شنود مجازی رسانه* یا VCS استفاده می‌شود. در این روش ایستگاه فرستنده ابتدا یک بسته کنترلی موسوم به تقاضای ارسال حاوی نشانی فرستنده، نشانی گیرنده، و زمان مورد نیاز برای اشغال کانال رادیویی را می‌فرستد. هنگامی که گیرنده این فریم را دریافت می‌کند، رسانه را کنترل می‌کند و در صورتی که رسانه آزاد باشد فریم کنترلی CTS را به نشانی فرستنده ارسال می‌کند. تمام ایستگاه‌هایی که فریم‌های کنترلی RTS/CTS را دریافت می‌کنند وضعیت کنترل رسانه خود موسوم به شاخص NAV را تنظیم می‌کنند. در صورتی که سایر ایستگاه‌ها بخواهند فریمی را ارسال کنند علاوه بر کنترل فیزیکی رسانه (کانال رادیویی) به پارامتر NAV خود مراجعه می‌کنند که مرتباً به صورت پویا تغییر می‌کند. به این ترتیب مشکل روزنه‌های پنهان حل شده و تصادم‌ها نیز به حداقل مقدار می‌رسند. شکل ۲-٤ زمان‌بندی RTS/CTS و وضعیت سایر ایستگاه‌ها را نشان می‌دهد.



شکل ۲-٤- زمان‌بندی RTS/CTS

لایه فیزیکی

در این استاندارد لایه فیزیکی سه عملکرد مشخص را انجام می‌دهد. اول آنکه رابطی برای تبادل فریم‌های لایه MAC جهت ارسال و دریافت داده‌ها فراهم می‌کند. دوم اینکه با استفاده از روش‌های تسهیم فریم‌های داده را ارسال می‌کند و در نهایت وضعیت رسانه (کانال رادیویی) را در اختیار لایه بالاتر (MAC) قرار می‌دهد.

سه تکنیک رادیویی مورد استفاده در لایه فیزیکی این استاندارد به شرح زیر می‌باشند:

- استفاده از تکنیک رادیویی DSSS
- استفاده از تکنیک رادیویی FHSS
- استفاده از امواج رادیویی مادون قرمز

در این استاندار لایه فیزیکی می‌تواند از امواج مادون قرمز نیز استفاده کند. در روش ارسال با استفاده از امواج مادون قرمز، اطلاعات باینری با نرخ ۱ یا ۲ مگابیت در ثانیه و به ترتیب با استفاده از مدولاسیون ۱۶-PPM و ٤-PPMمبادله می‌شوند.

ویژگی‌های سیگنال‌های طیف گسترده

عبارت طیف گسترده به هر تکنیکی اطلاق می‌شود که با استفاده از آن پهنای باند سیگنال ارسالی بسیار بزرگ‌تر از پهنای باند سیگنال اطلاعات باشد. یکی از سوالات مهمی که با در نظر گرفتن این تکنیک مطرح می‌شود آن است که با توجه به نیاز روز افزون به پهنای باند و اهمیت آن به عنوان یک منبع با ارزش، چه دلیلی برای گسترش طیف سیگنال و مصرف پهنای باند بیشتر وجود دارد. پاسخ به این سوال در ویژگی‌های جالب توجه سیگنال‌های طیف گسترده نهفته است. این ویژگی‌های عبارتند از:

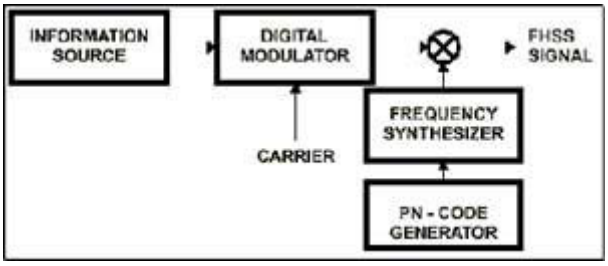
- پایین بودن توان چگالی طیف به طوری که سیگنال اطلاعات برای شنود غیر مجاز و نیز در مقایسه با سایر امواج به شکل اعوجاج و پارازیت به نظر می‌رسد.

- مصونیت بالا در مقابل پارازیت و تداخل
- رسایی با تفکیک پذیری و دقت بالا
- امکان استفاده در CDMA

مزایای فوق کمیسیون FCC را بر آن داشت که در سال ۱۹۸۵ مجوز استفاده از این سیگنال‌ها را با محدودیت حداکثر توان یک وات در محدوده ISM صادر نماید.

سیگنال‌های طیف گسترده با جهش فرکانسی

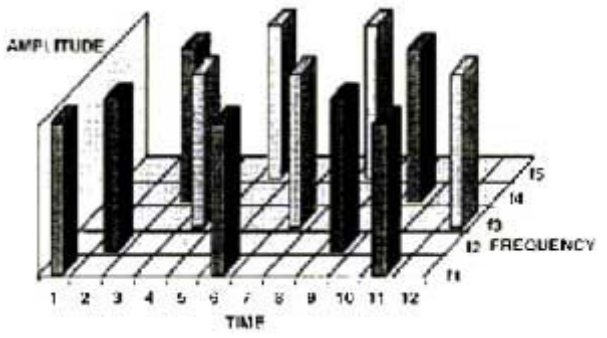
در یک سیستم مبتنی بر جهش فرکانسی، فرکانس سیگنال حامل به شکلی شبه تصادفی و تحت کنترل یک ترکیب کننده تغییر می‌کند. شکل ۲-۵ این تکنیک را در قالب یک نمودار نشان می‌دهد.



PN-CODE= Pseudonoise code

شکل ۲-۵ - تکنیک FHSS

در این شکل سیگنال اطلاعات با استفاده از یک تسهیم کننده دیجیتال و با استفاده از روش تسهیم FSK تلفیق می‌شود. فرکانس سیگنال حامل نیز به شکل شبه تصادفی از محدوده فرکانسی بزرگ‌تری در مقایسه با سیگنال اطلاعات انتخاب می‌شود. با توجه به اینکه فرکانس‌های pn-code با استفاده از یک ثبات انتقالی همراه با پس خور ساخته می‌شوند، لذا دنباله فرکانسی تولید شده توسط آن کاملا تصادفی نیست و به همین خاطر به این دنباله، شبه تصادفی می‌گوییم.



شکل ۲-٦- تغییر فرکانس سیگنال تسهیم شده به شکل شبه تصادفی

بر اساسی مقررات FCC و سازمان‌های قانون گذاری، حداکثر زمان توقف در هر کانال فرکانسی ٤٠٠ میلی ثانیه است که برابر با حداقل ۲,۵ جهش فرکانسی در هر ثانیه خواهد بود. در استاندارد ۸۰۲,۱۱ حداقل فرکانس جهش در آمریکای شمالی و اروپا ٦ مگاهرتز و در ژاپن ۵ مگاهرتز می‌باشد.-

سیگنال‌های طیف گسترده با توالی مستقیم

اصل حاکم بر توالی مستقیم، پخش یک سیگنال برروی یک باند فرکانسی بزرگتر از طریق تسهیم آن با یک امضاء یا کُد به گونه‌ای است که نویز و تداخل را به حداقل برساند. برای پخش کردن سیگنال هر بیت واحد با یک کُد تسهیم می‌شود. در گیرنده نیز سیگنال اولیه با استفاده از همان کد بازسازی می‌گردد. در استاندارد ۸۰۲,۱۱ روش مدولاسیون مورد استفاده در سیستم‌های DSSS روش تسهیم DPSK است. در این روش سیگنال اطلاعات به شکل تفاضلی تهسیم می‌شود. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد.

از آنجا که در استاندارد ۸۰۲,۱۱ و سیستم DSSS از روش تسهیم DPSK استفاده می‌شود، داده‌های خام به صورت تفاضلی تسهیم شده و ارسال می‌شوند و در گیرنده نیز یک آشکار ساز تفاضلی سیگنال‌های داده را دریافت می‌کند. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد. در روش تسهیم PSK فاز سیگنال حامل با توجه به الگوی بیتی سیگنال‌های داده تغییر می‌کند. به عنوان مثال در تکنیک QPSK دامنه سیگنال حامل ثابت است ولی فاز آن با توجه به بیت‌های داده تغییر می‌کند. جدول زیر ایده مدولاسیون فاز را نشان می‌دهد.

Symbols	Bits	Phase Modulation
١	٠٠	$A\sin(\omega t+\theta_1)$
٢	٠١	$A\sin(\omega t+\theta_2)$
٣	١٠	$A\sin(\omega t+\theta_3)$
٤	١١	$A\sin(\omega t+\theta_4)$

جدول ۲-۲- مدولاسیون فاز

در الگوی مدولاسیون QPSK چهار فاز مختلف مورد استفاده قرار می‌گیرند و چهار نماد را پدید می‌آورند. واضح است که در این روش تسهیم، دامنه سیگنال ثابت است. در روش تسهیم تفاضلی سیگنال اطلاعات با توجه به میزان اختلاف فاز و نه مقدار مطلق فاز تسهیم و مخابره می‌شوند. به عنوان مثال در روش pi/٤-DQPSK، چهار مقدار تغییر فاز ۳ -pi/٤، ۳pi/٤، pi/٤، و-pi/٤ است. با توجه به اینکه در روش فوق چهار تغییر فاز به کار رفته است لذا هر نماد می‌تواند دو بیت را کُدگذاری نماید.

اختلاف فاز	بیتهای زوج	بیتهای فرد
-۳pi/٤	۱	۱
۳ pi/٤	۱	۰
Pi/٤	۰	۰
-pi/٤	۰	۱

جدول ۲-۳- مدولاسیون تفاضلی

در روش تسهیم طیف گسترده با توالی مستقیم مشابه تکنیک FH از یک کد شبه تصادفی برای پخش و گسترش سیگنال استفاده می‌شود. عبارت توالی مستقیم از آنجا به این روش اطلاق شده است که در آن سیگنال اطلاعات مستقیماً توسط یک دنباله از کدهای شبه تصادفی تسهیم می‌شود. در این تکنیک نرخ بیتی شبه کُد تصادفی، نرخ تراشه نامیده می‌شود. در استاندارد ۸۰۲,۱۱ از کُدی موسوم به کُد *بارکر* برای تولید کدها تراشه سیستم DSSS استفاده می‌شود. مهم‌ترین ویژگی کدهای بارکر خاصیت غیر تناوبی و غیر تکراری آن است که به واسطه آن یک فیلتر تطبیقی دیجیتال قادر است به راحتی محل کد بارکر را در یک دنباله بیتی شناسایی کند.

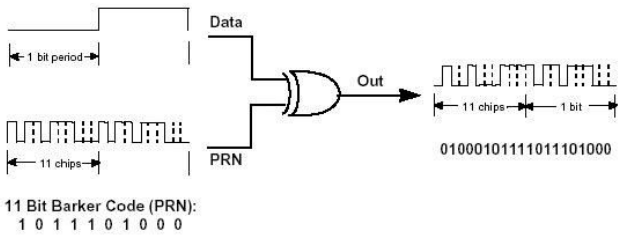
جدول زیر فهرست کامل کدهای بارکر را نشان می‌دهد. همانگونه که در این جدول مشاهده می‌شود کدهای بارکر از ۸ دنباله تشکیل شده است. در تکنیک DSSS که در استاندارد ۸۰۲,۱۱ مورد استفاده قرار می‌گیرد، از کد بارکر با

طول ۱۱ (N=۱۱) استفاده می‌شود. این کد به ازاء یک نماد، شش مرتبه تغییر فاز می‌دهد و این بدان معنی است که سیگنال حامل نیز به ازاء هر نماد ٦ مرتبه تغییر فاز خواهد داد.

CODE LENGTH (N)	BARKER SEQUENCE
1	+
2	+ + or + -
3	+ + -
4	+ + + - or + + - +
5	+ + + - +
7	+ + + - - + -
11	+ + + - - - + - - + -
13	+ + + + + - - + + - + - +

جدول ۲-٤- کدهای بارکر

لازم به یادآوری است که کاهش پیچیدگی سیستم ناشی از تکنیک تسهیم تفاضلی DPSK به قیمت افزایش نرخ خطای بیتی به ازاء یک نرخ سیگنال به نویز ثابت و مشخص است.

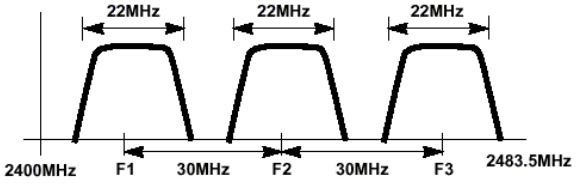


شکل۲-۷- مدار مدولاسیون با استفاده از کدهای بارکر

شکل ۲-۷ مدل منطقی مدولاسیون و پخش سیگنال اطلاعات با استفاده از کدهای بارکر را نشان می‌دهد.

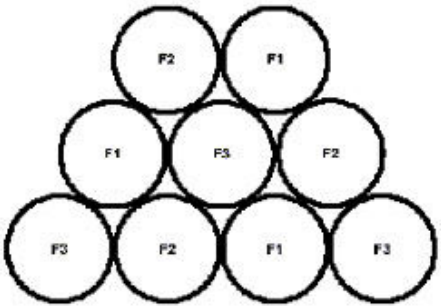
استفاده مجدد از فرکانس

یکی از نکات مهم در طراحی شبکه‌های بی‌سیم، طراحی شبکه سلولی به گونه‌ای است که تداخل فرکانسی را تا جای ممکن کاهش دهد. شکل ۲-۸ سه کانال DSSS در محدوده فرکانسی ISM را نشان می‌دهد.



شکل ۲-۸- سه کانال فرکانسی F۳,F۲,F۱

شکل ۲-۹ مفهوم استفاده مجدد از فرکانس با استفاده از شبکه‌های مجاور فرکانسی را نشان می‌دهد. در این شکل مشاهده می‌شود که با استفاده از یک طراحی شبکه سلولی خاص، تنها با استفاده از سه فرکانس متمایز F۱,F۲,F۳ امکان استفاده مجدد از فرکانس فراهم شده است.



شکل ۲-۹- طراحی شبکه سلولی

در این طراحی به هریک از سلول‌های همسایه یک کانال متفاوت اختصاص داده شده است و به این ترتیب تداخل فرکانسی بین سلول‌های همسایه به حداقل رسیده است. این تکنیک همان مفهومی است که در شبکه تلفنی سلولی یا شبکه تلفن همراه به کار می‌رود. نکتهجالب دیگر آن است که این شبکه سلولی به راحتی قابل گسترش است. خوانندگان علاقمند می‌توانند دایره‌های جدید را در چهار جهت شبکه سلولی شکل فوق با فرکانس‌های متمایز F۱,F۲,F۳ ترسیم و گسترش دهند.

آنتن‌ها

در یکی تقسیم بندی کلی آنتن‌های مورد استفاده در استاندارد IEEE ۸۰۲,۱۱ به دو دسته: تمام جهت و نقطه به نقطه تقسیم می‌شوند. واضح است که آنتن‌های تمام جهته با توجه به آنکه نیازی به تنظیم ندارند، راحت‌تر مورد استفاده قرار می‌گیرند. این آنتن‌ها در اغلب کارت‌های شبکه (کارت‌های دسترسی) و نیز نقاط دسترسی یا ایستگاه‌های پایه بکار می‌روند.

این آنتن‌ها در فواصل کوتاه قابل استفاده هستند و برای بهره گیری در فواصل طولانی‌تر به تقویت کننده‌های خارجی نیاز دارند که البته در بسیاری موارد استفاده از این تقویت کننده‌های خارجی میسر و یا قانونی نیست. از سوی دیگر آنتن‌های نقطه به نقطه یا خطی در کاربردهای خارجی استفاده می‌شوند و به تنظیم دقیق نیاز دارند.

محدوده عملیاتی رایج در آنتن‌های تمام جهته ٤٥ متر و محدوده عملیاتی آنتنهای نقطه به نقطه و توان بالا در حدود ٤٠ کیلومتر است. در کاربردهایی که استفاده از تقویت کننده بلا مانع است، این محدوده عملیاتی به شکل قابل توجهی افزایش یافته و تنها توسط خط دید (مسیر دید) محدود می‌شود. از جمله عوامل مهمی که محدوده عملیاتی تجهیزات مبتنی بر IEEE ۸۰۲,۱۱ را تحت تأثیر قرار می‌دهد محل نصب نقاط دسترسی یا ایستگاه پایه و نیز تداخل رادیویی است. همانگونه که پیشتر گفته شد، تجهیزات مبتنی بر این استاندارد سعی می‌کنند که با بالاترین نرخ ارسال داده کار کنند و در صورت نیاز به سرعت‌های پایین‌تر برگردند.

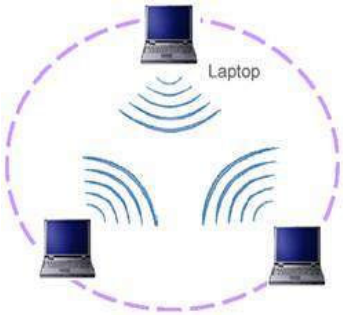
نتیجه:

استاندارد ۸۰۲,۱۱b به تجهیزات اجازه می‌دهد که به دو روش ارتباط در شبکه برقرار شود. این دو روش عبارت‌اند از برقراری ارتباط به صورت نقطه به نقطه –همان‌گونه در شبکه‌های Ad hoc به‌کار می‌رود– و اتصال به شبکه از طریق نقاط تماس یا دسترسی (AP=Access Point).

معماری معمول در شبکه‌های محلی بی‌سیم بر مبنای استفاده از AP است. با نصب یک AP، عملاً مرزهای یک سلول مشخص می‌شود و با روش‌هایی می‌توان یک سخت‌افزار مجهز به امکان ارتباط بر اساس استاندارد ۸۰۲,۱۱b را میان سلول‌های مختلف حرکت داد. گستره‌یی که یک AP پوشش می‌دهد را BSS(Basic Service Set) می‌نامند. مجموعه‌ی تمامی سلول‌های یک ساختار کلی شبکه، که ترکیبی از BSSهای شبکه است، را ESS(Extended Service Set) می‌نامند. با استفاده از ESS می‌توان گستره‌ی وسیع‌تری را تحت پوشش شبکه‌ی محلی بی‌سیم درآورد.

در سمت هریک از سخت‌افزارها که معمولاً مخدوم هستند، کارت شبکه‌یی مجهز به یک مودم بی‌سیم قرار دارد که با AP ارتباط را برقرار می‌کند. AP علاوه بر ارتباط با چند کارت شبکه‌ی بی‌سیم، به بستر پرسرعت‌تر شبکه‌ی سیمی مجموعه نیز متصل است و از این طریق ارتباط میان مخدوم‌های مجهز به کارت شبکه‌ی بی‌سیم و شبکه‌ی اصلی برقرار می‌شود.

همان‌گونه که گفته شد، اغلب شبکه‌های محلی بی‌سیم بر اساس ساختار فوق، که بـه نـوع Infrastructure نیـز موسوم است، پیاده‌سازی می‌شوند. با این وجود نوع دیگری از شبکه‌های محلی بی‌سیم نیز وجود دارند که از همـان منطق نقطه‌به‌نقطه استفاده می‌کنند. در این شبکه‌ها که عموماً Ad hoc نامیده می‌شوند یـک نقطـه‌ی مرکـزی بـرای دسترسی وجود ندارد و سخت‌افزارهای همراه – مانند کامپیوترهای کیفی و جیبی یا گوشی‌های موبایـل – بـا ورود به محدوده‌ی تحت پوشش این شبکه، به دیگر تجهیزات مشابه متصل می‌گردند. این شبکه‌ها به بستر شبکه‌ی سیمی متصل نیستند و به همین منظور IBSS (Independent Basic Service Set) نیز خواند می‌شـوند. شـکل زیر شمایی ساده از یک شبکه‌ی Ad hoc را نشان می‌دهد :



شبکه‌های Ad hoc از سویی مشابه شبکه‌های محلی درون دفتر کار هستند که در آنها نیازی به تعریف و پیکربندی یک سیستم رایانه‌یی به عنوان خادم وجود ندارد. در این صورت تمامی تجهیزات متصل بـه ایـن شـبکه مـی‌تواننـد پرونده‌های مورد نظر خود را با دیگر گره‌ها به اشتراک بگذارند

شبکه های اطلاعاتی

یک مدل مناسب برای تجزیه و تحلیل یک شبکه اطلاعاتی، مدل

OSI (Open System Interconnection) تشکیل شده از ۷ لایه است که کنترل شبکه را به عهده دارند.

۱) Physical Layer

۲)Data Link Layer

۳)Network Layer

٤)Transport Layer

٥)Session Layer

٦)Presentation Layer

۷)Application Layer

۸۰۲ . ۱۱ (لایه های)

استاندارد IEEE ۸۰۲,۱۱ در ۱۹۹۷ June برای WLAN ها منتشر شد. در این استاندارد فقط درباره ی دو لایه ی PHY و MAC صحبت شده است.

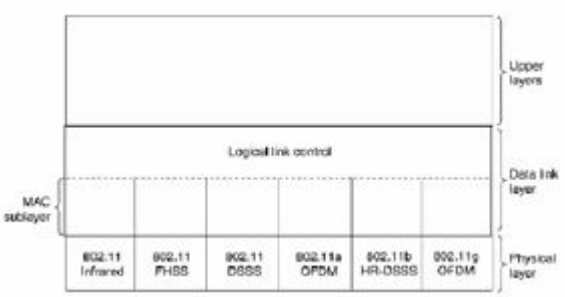


Fig ۱. ۸۰۲,۱۱ Protocol Stack

لایه اول: Physical Layer . این لایه مستقیما در رابطه با ارسال و دریافت سیگنال و تکنیک ها و سخت افزار لازم برای این کار است (مثلا فیبر نوری در شبکه های مخابراتی نوری یا کابل مسی در شبکه تلفن).

لایه دوم: Data Link Layer. مسئولیت اصلی این لایه مدیریت و کنترل بسته های اطلاعاتی (packets) است. مفاهیمی مانند کنترل خطا و پروتکل ها به این لایه مربوط است. این لایه خود از دو زیر لایه (sub (MAC) Medium Access Control layer)، که کنترل اجازه دسترسی (Access) به اطلاعا ت

و زیـر لایـه Logical Link Control، کـه وظیفـه همزمـان ارسـال شـدن اطلاعـات و کنتـرل خطـا (error checking)، و پنهان کردن تفاوتهای استانداردهای مختلف از لایه های بالاتر شبکه را به عهده دارد.

محدوده فرکانسی ارسال دیتـا در بانـد آزاد ISM ۲,٤ GHz (Industrial Scientific and Medical)و نرخ ارسال بین ۱ تا ۲ Mbps است.

۸۰۲,۱۱ از دو مکانیزم متفـاوت ارسـال رادیـویی در لایـه PHY خـود اسـتفاده مـی کنـد. روش هـای DSSS (Direct Sequence Spread Spectrum) و FHSS (Frequency Hopped Spread Spectrum) و یک مکانیزم ارسال بوسیله مادون قرمز. اما چون در روش مادون قرمز پهنای باند کوچک اسـت ازاین روش کمتر استفاده می شود.

در دو روش اول ، سیگنال مورد نظر ارسالی به طوری تغییر شکل داده می شود که در حالیکـه انـرژی کـل سـیگنال ثابت است، محدوده فرکانسی بیشتری را اشغال می کند تا از اطمینان ارسال بیشتری برخوردار باشد.

در لایه MAC ۸۰۲,۱۱ دو حالت برای ارتباطات درون شبکه تعریف می شود:

۱)DCF (Distributed Coordination Function)

۲)PCF (Point Coordination Function)

DCF که استاندارد موظف است آن را پشتیبانی کنـد، تـا قابلیتهـای Ethernet را داشـته باشـد، وقتـی اسـت کـه Station ها بتوانند با یکدیگر به طور بی واسطه ارتباط داشته باشند. حالت دیگر یعنی PCF وقتی است که همـه Station ها به واسطه یک base Station با هم مرتبط هستند. در این مد، چون همـه چیـز بـا واسـطه اسـت، base Station می تواند به Station ها نوبت برای ارسال اطلاعات خود دهد و بدین صورت مـشکلی پـیش نمی آید. ولی در DCF چنین امکانی وجود ندارد و برای جلوگیری از برخورد اطلاعات فرسـتاده شـده بایـد فکـر دیگری کرد. طبیعی است که در شبکه سیار موانع و مسائلی که باید حل شود به مراتب پیچیـده تـر از Ethernet است که در آن یک محیط پایدار بـرای تبـادل اطلاعـات وجـود دارد مـی باشـند. بـرای مثـال در Ethernet هـر

Station به سادگی می تواند هر Station را ببیند، ولی در شبکه های سیار مشکل Range محدود فرستنده های رادیویی وجود دارد و لزوما همه Station ها نمی توانند از فعالیتهای هم باخبر باشند.روشی که بدین منظور استفاده می شود CSMA/CA(Carrier Sense Multiple Access with Collision Avoidence) است.

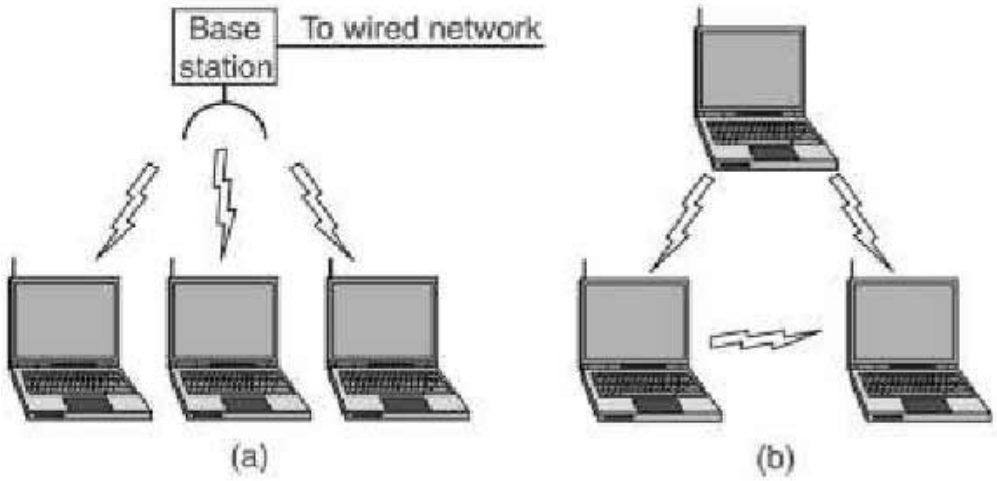


Fig ۱. DCF & PCF operation: a) PCF b)DCF

با دو روش Authentication و Encryption امنیت رد و بدل اطلاعات را بالا می برد.authentication یعنی دادن اجازه ارسال و دریافت اطلاعات به وسیله یک Station به Station های دیگر. این در صورتی است که Station ها دو به دو با هم مرتبط باشند. اصطلاحا به این روش ارتباط Station ها روش IBSS (Independent Basic Service Set) گفته می شود. اگر Station ها از طریق یک Access Point با هم در ارتباط با شند یک Set Infrastructure Basic Service تشکیل می شود. با ارتباط چند BSS Infrastructure به هم از طریق یک Distribution System (که معمولا یک شبکه wired مثل Ethernet LAN است.) یک شبکه گسترده تر به نام ESS (Extended Service Set) به وجود می آید.

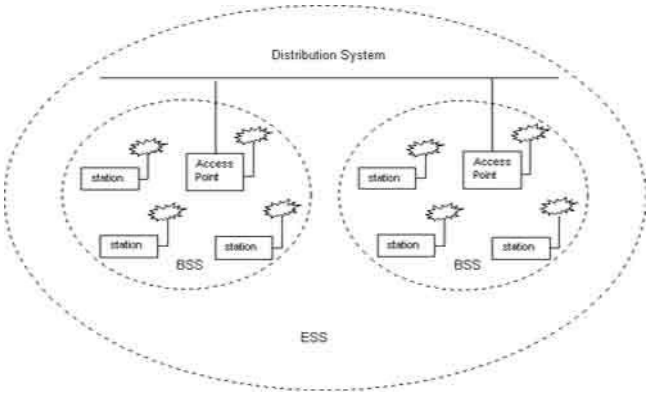


Fig۱. Extended Service Set (ESS)

Wifi چگونه کار می کند؟

فناوری wifi یا ۸۰۲,۱۱ بسیار شبیه به گوشی تلفن دیجیتال بیسیم کار می کند.میکروفون موجود در گوشی صدای شما را می گیرد و پردازنده درونی این گوشی این صدا را به یک سیگنال دیجیتال تبدیل می کند که سپس به دستگاه پایه انتقال می یابد. دستگاه پایه به نوبه خود داده هایی که از خط تلفن می اید می گیرد و یک تبدیل مشابه انجام میدهد و سیگنا حاصل را به گوشی می فرستد .این ارتباط دو طرفه پیوسته تا حدودی به ملیات یک شبکه بیسیم شباهت دارد .یک دستگاه wap (نقطه دست بی سیم) یا دستگاه مسیر یابی بی سیم را می توانید همان دستگاه پایه گوشی تلفن و کارتهای شبکه بیسیم را خود گوشی در نظر بگیرید . wap یا مسیر یاب رابط با سیم به یک شبکه باسیم موجود یا به یک مودم باند عریض است و با استفاده از سیگنالهای رادیویی با کارتهای شبکه

بی سیم نصب شده در کامپیوتر های شما ارتباط بر قرار می کنند.

برای درک بهتر و ساده یک شبکه بیسیم یک جفت دستگاه رادیویی ترانزیستوری کوچک(walkie-talkie) پنج دلاری در نظر بگیرید

پیوند بی سیم بین کارتهای نصب شده در کامپیوتر های شما و مسیر یاب wap نیاز به کابلهای اترنت را بر طرف می کند. واکی تاکی دستگاه رادیویی کوچک است که می تواند سیگنا لهای رادیویی را ارسال و دریافت کند .زمانی که شما با این دستگاه صحبت می کنید صدای شما توسط میکروفن در یافت می شود و رد یک فرکانس رادیویی کد گذاری می شود و توسط آنتن ارسال می شود.

یک رادیوی مشابه دیگر می تواند این مخابره را به وسیله آنتن خود دریافت کند رمز صدای شما را از سیگنا رادیویی بردارد و صدا را توسط بلندگو بشنود.چنین دستگاه های مخابره ساده ای

سیگنال هایی با قدرت ۰/۲۵ وات ارسال می کند و می توانند تا حدود ۵۰۰ تا ۱۰۰۰ فوت مخابره کنند . تصور کنید که می خواهید دو کامپیوتر را در شبکه با استفاده از این تکنولوژی به یکدیگر متصل کنید .این سیستم کار خواهد

کرد اما سرعت انتقال اطلاعات بسیار کند است . یک دستگاه کوچک پنج دلاری برای صدای انسان طراحی شده است بنابراین شما نمی توانید اطلاعات بسیار زیادی را با استفاده از این روش ارسال کنید.

برای استفاده از این سیستم ایستگاه هایی به نام point Access در مناطق مختلف و به فواصل چند صد متری قرار می گیرد. این ایستگاه ها امواج رادیویی را در هوا منتشر می کنند و هر کامپیوتری که به Wi-Fi مجهز باشد و در محدوده این ایستگاه ها قرار داشته باشد قادر به استفاده از اینترنت است و کاربران با قرار دادن یک کارت سخت افزاری IEEE۸۰۲,۱۱b و یا وصل کردن یک دستگاه Wi-Fi اکسترنال از طریق USB به کامپیوتر خود قادر به استفاده از این سیستم هستند. قیمت اینترنت در این سیستم بسیار مناسب است. مثلاً در کشور آمریکا یک Account نامحدود یک ماهه با این سرویس به مبلغ ۲۰ تا ۳۰ دلار در اختیار کاربران قرار می گیرد. از نظر برد موثر هم حداکثر تا ۱۵۰ متر اطراف Access Point مورد پوشش قرار می گیرد. در این حالت سرعت انتقال ارتباط ۱mbps است. البته هر چقدر فاصله کاربر با ایستگاه اصلی کمتر از ۱۵۰ متر باشد سرعت انتقال اطلاعات بیشتر خواهد شد. مثلاً سرعت انتقال اطلاعات در فاصله ۱۰۰ متری ۵,۵mbps، در فاصله ۸۰ متری ۸mbps و در فاصله ۵۰ متری و کمتر از آن ۱۱mbps است .

فقط کامپیوتر خود را روشن کنید!

یکی از مهمترین مزایای وای فای سادگی آن است.در بسیاری از لپ تاپ های جدید یک کارت وای فای قرار دارد و در بیشتر موارد نیازی نیست تا شما برای شروع استفاده از وای فای کاری انجام دهید .همچنین اضافه کردن کارت به لپ تاب های قدیمی تر یا یک کامپیوتر رومیزی بسیار آسان است .

Hotspot یک نقطه ارتباطی برای شبکه وای فای است. Hotspot یک جعبه کوچک است که حاوی یک کارت ۸۰۲/۱۱ است و می تواند به طور همزمان با بیشتر از صد کارت ۸۰۲/۱۱ ارتباط بر قرار کند .در حال حاضر تعداد بسیار زیادی از این نقاط ارتباطی وای فای در مکان های عمومی مانند رستوران ها وهتل ها و کتابخانه ها و فرودگاه ها وجود دارد شما همچنین می توانید یک Hotspot در منزلتان ایجاد کنید.

در ماشین های جدید یک کارت۸۰۲/۱۱ به طور خودکار به یک ۸۰۲/۱۱hotsopt متصل می شود و ارتباط با شبکه برقرار می شود. به محض اینکه شما کامپیوترتان را روشن کنید به شبکه متصل می شوید و شما می توانید ای میل خودتان را چک کنید و با اینترنت کارکنید.در تجهیزات۸۰۲/۱۱ قدیمی خصوصیت جستجوی خوکار وجود ندارد. در این حالت شما باید یک لغت که SSID نامیده می شود (معمولا یک کلمه کوتاه حداکثر با ۱۰ کلمه)و شماره کانال که عدد صحیحی بین صفر و یازدهاست را بیابدو این دو را تایپ کند.در مدل های جدیدتر که به طور خوکار عمل می کنند این دو بخش اطلاعات از سیگنالهای رادیویی تولید شده توسطhotsopt گرفته می شودو برای شما نمایش داده می شود.

IEEE ۸۰۲.۱۱

امروزه با بهبود عملکرد، کارایی و عوامل امنیتی، شبکه‌های بی‌سیم به شکل قابل توجهی در حال رشد و گسترش هستند و استاندارد IEEE ۸۰۲,۱۱ استاندارد بنیادی است که شبکه‌های بی‌سیم بر مبنای آن طراحی و پیاده سازی می‌شوند.

۸۰۲,۱۱ از استانداردهای پیاده سازی شبکه های بیسیم می باشد که توسط IEEE ارائه شده است. این استاندارد شبیه استاندارد ۸۰۲,۳ روی Ethernetنودهای شبکه بیسم نیز توسط آدرس MAC حک شده روی کارت های شبکه آدرس دهی می شوند. اگر چه ۸۰۲,۱۱ از سیم به عنوان رسانه در لایه ۱ استفاده نمی کند و نودها در استاندارد فوق به صورت بیسیم و در دامنه ای که توسط دستگاهای بیسیم تعریف می شوند با یکدیگر تبادل اطلاعات می نمایند.

استاندارد ۱۹۹۷، پهنای باند Mbps۲ را تعریف می‌کند با این ویژگی که در شرایط نامساعد و محیط‌های دارای اغتشاش (نویز) این پهنای باند می‌تواند به مقدار Mbps۱ کاهش یابد. روش تلفیق یا مدولاسیون در این پهنای باند روش DSSS است. بر اساس این استاندارد پهنای باند Mbps ۱ با استفاده از روش مدولاسیون FHSS نیز قابل دستیابی است و در محیط‌های عاری از اغتشاش (نویز) پهنای باند Mbps ۲نیز قابل استفاده است. هر دو روش مدولاسیون در محدوده باند رادیویی GHz ۲,٤ عمل می‌کنند. یکی از نکات جالب توجه در خصوص این استاندارد استفاده از رسانه مادون قرمز علاوه بر مدولاسیون‌های رادیویی DSSS و FHSS به عنوان رسانهانتقال است. ولی کاربرد این رسانه با توجه به محدودیت حوزه عملیاتی آن نسبتاً محدود و نادر است. گروه کاری ۸۰۲,۱۱ به زیر گروه‌های متعددی تقسیم می‌شود. شکل‌های ۱-۱ و ۱-۲ گروه‌های کاری فعال در فرآیند استاندارد سازی را نشان می‌دهد. برخی از مهم‌ترین زیر گروه‌ها به قرار زیر است:

- ۸۰۲,۱۱D: Additional Regulatory Domains

- ۸۰۲,۱۱E: Quality of Service (QoS)

- ۸۰۲,۱۱F: Inter-Access Point Protocol (IAPP)

- ۸۰۲,۱۱G: Higher Data Rates at ۲,٤ GHz

- ۸۰۲,۱۱H: Dynamic Channel Selection and Transmission Power Control

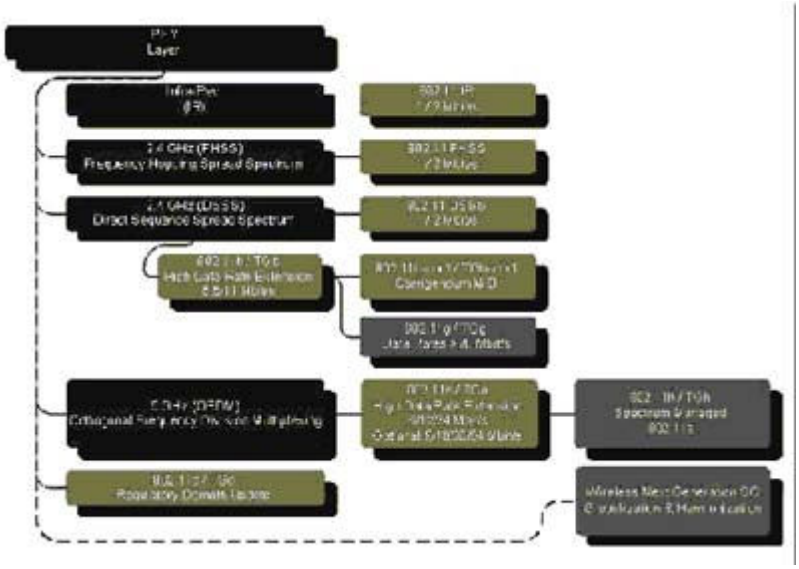
- ۸۰۲,۱۱i: Authentication and Security

کمیته e۸۰۲,۱۱ کمیته‌ای است که سعی دارد قابلیت QoS اِتـرنت را در محیط شبکه‌های بی‌سیم ارائه کنـد. توجـه داشته باشید که فعالیت‌های این گروه تمام گونه‌های ۸۰۲,۱۱ شامل a، b، و g را در بر دارد. این کمیته در نظر دارد که ارتباط کیفیت سرویس سیمی یا Ethernet QoS را به دنیای بی‌سیم بیاورد.

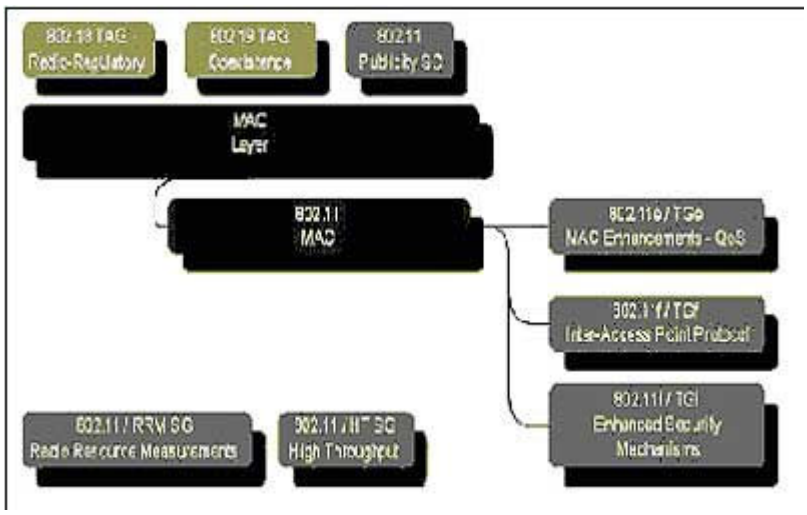
کمیته g۸۰۲,۱۱ کمیته‌ای است که با عنوان ۸۰۲,۱۱ توسعه یافته نیز شناخته می‌شود. ایـن کمیتـه در نظـر دارد نـرخ ارسال داده‌ها در باند فرکانسی ISM را افزایش دهد. باند فرکانسی ISM یـا باننـد فرکانـسی صـنعتی، پژوهـشی، و پزشکی، یک باند فرکانسی بدون مجوز است. استفاده از این باند فرکانسی که در محدوده ۲٤۰۰ مگاهرتز تا ۲٤۸۳,۵ مگاهرتز قرار دارد، بر اساس مقررات FCC در کاربردهـای تشعـشع رادیـویی نیـازی بـه مجـوز نـدارد. اسـتاندارد g۸۰۲,۱۱ تا کنون نهایی نشده است و مهم‌ترین علت آن رقابت شدید میان تکنیک‌های مدولاسـیون اسـت. اعـضاء این کمیته و سازندگان تراشه توافق کرده‌اند که از تکنیک تسهیم OFDM استفاده نمایند ولی بـا ایـن وجـود روش PBCC نیز می‌تواند به عنوان یک روش جایگزین و رقیب مطرح باشد.

کمیته h۸۰۲,۱۱ مسئول تهیه استانداردهای یکنواخت و یکپارچه برای توان مصرفی و نیز توان امواج ارسالی توسـط فرستنده‌های مبتنی بر ۸۰۲,۱۱ است.

فعالیت دو کمیته i۸۰۲,۱۱ و x۸۰۲,۱۱ در ابتدا برروی سیستم‌های مبتنی بر b۸۰۲,۱۱ تمرکز داشت. ایـن دو کمیتـه مسئول تهیه پروتکل‌های جدید امنیت هستند. استاندارد اولیه از الگوریتمی موسوم به WEP استفاده می‌کنـد کـه در آن دو ساختار کلید رمز نگاری به طول ٤۰ و ۱۲۸ بیت وجود دارد. WEP مشخصاً یک روش رمزنگاری است کـه از الگوریتم RC٤ برای رمزنگاری فریم‌ها استفاده مـی‌کنـد. فعالیـت ایـن کمیتـه در راسـتای بهبـود مـسائل امنیتـی شبکه‌های محلی بی‌سیم است.



شکل ۱-۱- گروه‌های کاری لایه فیزیکی



شکل ۱-۲- گروه‌های کاری لایه دسترسی به رسانه

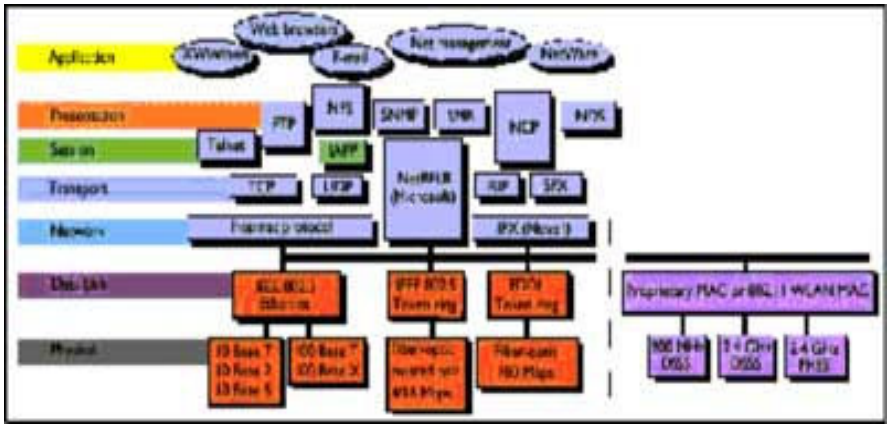
این استاندارد لایه‌های کنترل دسترسی به رسانه (MAC) و لایه فیزیکی (PHY) در یک شبکه محلی با اتصال بی‌سیم را دربردارد. شکل ۱-۳ جایگاه استاندارد ۸۰۲,۱۱ را در مقایسه با مدل مرجع نشان می‌دهد.

شکل ۱-۳- مقایسه مدل مرجع OSI و استاندارد ۸۰۲,۱۱

محیط‌های بی‌سیم دارای خصوصیات و ویژگی‌های منحصر به فردی می‌باشند که در مقایسه با شبکه‌های محلی سیمی جایگاه خاصی را به این گونه شبکه‌ها می‌بخشد. به طور مشخص ویژگی‌های فیزیکی یک شبکه محلی بی‌سیم محدودیت‌های فاصله، افزایش نرخ خطا و کاهش قابلیت اطمینان رسانه، همبندی‌های پویا و متغیر، تداخل امواج، و عدم وجود یک ارتباط قابل اطمینان و پایدار در مقایسه با اتصال سیمی است. این محدودیت‌ها، استاندارد شبکه‌های محلی بی‌سیم را وا می‌دارد که فرضیات خود را بر پایه یک ارتباط محلی و با بُرد کوتاه بنا نهد. پوشش‌های جغرافیایی وسیع‌تر از طریق اتصال شبکه‌های محلی بی‌سیم کوچک برپا می‌شود که در حکم عناصر ساختمانی شبکه گسترده هستند. سیّار بودن ایستگاه‌های کاری بی‌سیم نیز از دیگر ویژگی‌های مهم شبکه‌های محلی بی‌سیم است. در حقیقت اگر در یک شبکه محلی بی‌سیم ایستگاه‌های کاری قادر نباشند در یک محدودهعملیاتی قابل قبول و همچنین میان سایر شبکه‌های بی‌سیم تحرک داشته باشد، استفاده از شبکه‌های محلی بی‌سیم توجیه کاربردی مناسبی نخواهد داشت.

از سوی دیگر به منظور حفظ سازگاری و توانایی تطابق و همکاری با سایر استانداردها، لایه دسترسی به رسانه (MAC) در استاندارد ۸۰۲,۱۱ می‌بایست از دید لایه‌های بالاتر مشابه یک شبکه محلی مبتنی بر استاندارد ۸۰۲ عمل کند. بدین خاطر لایه MAC در این استاندارد مجبور است که سیّاربودن ایستگاه‌های کاری را به گونه‌ای شفاف پوشش دهد که از دید لایه‌های بالاتر استاندارد این سیّاربودن احساس نشود. این نکته سبب می‌شود که لایهMAC در این استاندارد وظایفی را بر عهده بگیرد که معمولاً توسط لایه‌های بالاتر شبکه انجام می‌شوند. در واقع این استاندارد لایه‌های فیزیکی و پیوند داده جدیدی به مدل مرجع OSI اضافه می‌کند و به طور مشخص لایه فیزیکی جدید از فرکانس‌های رادیویی به عنوان رسانهانتقال بهره می‌برد. شکل۱-٤، جایگاه این دو لایه در مدل مرجع OSI را در کنار سایر پروتکل‌های شبکه سازی نشان می‌دهد.

همانگونه که در این شکل مشاهده می‌شود وجود این دولایه از دید لایه‌های فوقانی شفاف است.



شکل ۱-٤- جایگاه ۸۰۲,۱۱ در مقایسه با سایر پروتکل‌ها

پذیرش استاندارد های WLAN از سوی کاربران

۸۰۲,۱۱b

۸۰۲,۱۱ b اولین نسخه ای بود که به بازار مصرف رسید و کندترین و ارزان قیمت ترین در بین این سه استاندارد محسوب می شود . .تا کنون استاندارد مورد استفاده در شبکه های بی سیم ۸۰۲,۱۱b بوده است. محصولات مبتنی بر ۸۰۲,۱۱b به عنوان اولین استاندارد رایج با مزایایی از قبیل سرعت قابل قبول ، قیمت مناسب ، سازگاری جهانی ، استفاده از طیف فرکانسی GHz ۲,٤(که نیازی به مجوز از ارگانهای دولتی ندارد)و همچنین یکپارچگی محصولات تحت نظارت اتحادیه Wi-Fi همه و همه موجب شده اند تا چیزی حدود ۹۵٪ از سهم بازار را به خود اختصاص دهند .

به طور سنتی این استانداردر از دو فنّاوری DSSS یا FHSS استفاده می‌کند. هر دو روش فوق برای ارسال داده با نرخ های ۱ و ۲ مگابیت در ثانیه مفید هستند.

جدول ۳-۱ سرعت مختلف قابل دسترسی در این استاندارد را نشان می‌دهد.

Bits/Symbol	Symbol Rate	Modulation	Code Length	Data Rate
۱	۱ MSps	BPSK	۱۱ (Barker Sequence)	۱ Mbps
۲	۱ MSps	QPSK	۱۱ (Barker Seq.)	۲ Mbps
٤	۱,۳۷۵ MSps	QPSK	۸ CCK	۵,۵ Mbps
۸	۱,۳۷۵ MSps	QPSK	۸ CCK	۱۱ Mbps

جدول ۳-۱- نرخ‌های ارسال داده در استاندارد b۸۰۲,۱۱

در ایالات متحده آمریکا کمیسیون فدرال مخابرات یا FCC، مخابره و ارسال فرکانس های رادیویی را کنترل می‌کند. این کمیسیون باند فرکانس خاصی موسوم به ISM را در محدوده ۲,٤ GHz تا ۲,٤۸۳۵ GHz برای فنّاوری‌های رادیویی استاندارد IEEE۳-۱-اثرات فاصله

فاصله از فرستنده برروی کارایی و گذردهی شبکه‌های بی‌سیم تاثیر قابل توجهی دارد. فواصل رایج در استاندارد ۸۰۲,۱۱ با توجه به نرخ ارسال داده تغییر می‌کند و به طور مشخص در پهنای باند ۱۱ Mbps این فاصله ۳۰ تا ٤۵ متر و در پهنای باند ۵,۵ Mbps، ٤۰ تا ٤۵ متر و در پهنای باند ۲ Mbps، ۷۵ تا ۱۰۷ متر است. لازم به یادآوری است که این فواصل توسط عوامل دیگری نظیر کیفیت و توان سیگنال، محل استقرار فرستنده و گیرنده و شرایط فیزیکی و محیطی تغییر می‌کنند.

در استاندارد b۸۰۲,۱۱ پروتکلی وجود دارد که گیرنده بسته را ملزم به ارسال بسته تصدیق می‌نماید (رجوع کنید به بخش ۲-٤ دسترسی به رسانه). توجه داشته باشید که این مکانیزم تصدیق علاوه بر مکانیزم‌های تصدیق رایج در سطح لایه انتقال (نظیر آنچه در پروتکل TCP اتفاق می‌افتد) عمل می‌کند. در صورتی که بسته تصدیق ظرف مدت

زمان مشخصی از طرف گیرنده به فرستنده نرسد، فرستنده فرض می‌کند که بسته از دست رفته است و مجدداً آن بسته را ارسال می‌کند. در صورتی که این وضعیت ادامه یابد نرخ ارسال داده نیز کاهش می‌یابد (Fall Back) تا در نهایت به مقدار ۱ Mpbs برسد. در صورتی که در این نرخ حداقل نیز فرستنده بسته‌های تصدیق را در زمان مناسب دریافت نکند ارتباط گیرنده را قطع شده تلقی کرده و دیگر بسته‌ای را برای آن گیرنده ارسال نمی‌کند. به این ترتیب فاصله ۸۰۲,۱۱b اختصاص داده است.

نقش مهمی در کارایی (میزان بهره‌وری از شبکه) و گذردهی (تعداد بسته های غیرتکراری ارسال شده در واحد زمان) ایفا می‌کند.

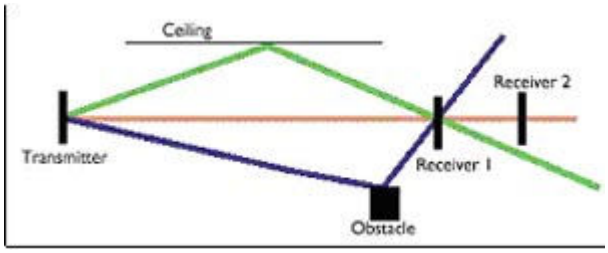
پل بین شبکه‌ای

بر خلاف انتظار بسیاری از کارشناسان شبکه‌های کامپیوتری، پل بین شبکه‌ای یا Bridging در استاندارد ۸۰۲,۱۱b پوشش داده نشده است. در پل بین شبکه‌ای امکان اتصال نقطه به نقطه (و یا یک نقطه به چند نقطه) به منظور برقراری ارتباط یک شبکه محلی با یک یا چند شبکه محلی دیگر فراهم می‌شود. این کاربرد به خصوص در مواردی که بخواهیم بدون صرف هزینه کابل کشی (فیبر نوری یا سیم مسی) شبکه محلی دو ساختمان را به یکدیگر متصل کنیم بسیار جذاب و مورد نیاز می‌باشد. با وجود اینکه استاندارد ۸۰۲,۱۱b این کاربرد را پوشش نمی‌دهد ولی بسیاری از شرکت‌ها پیاده‌سازی‌های انحصاری از پل بی‌سیم را به صورت گسترش و توسعه استاندارد ۸۰۲,۱۱b ارائه کرده‌اند. پل‌های بی‌سیم نیز توسط مقررات FCC کنترل می‌شوند و گذردهی مؤثر یا به عبارت دیگر توان مؤثر ساطع شده همگرا (EIRP) در این تجهیزات نباید از ٤ وات بیشتر باشد. بر اساس مقررات FCC توان سیگنال‌های ساطع شده در شبکه‌های محلی نیز نباید از ۱ وات تجاوز نماید.

پدیده چند مسیری

شکل ۳-۱ پدیده چند مسیری را نشان می‌دهد. در این پدیده مسیر و زمان بندی سیگنال در اثر برخورد با موانع و انعکاس تغییر می‌کند. پیاده سازی‌های اولیه از استاندارد ۸۰۲,۱۱b از تکنیک FHSS در لایه فیزیکی استفاده می‌کردند. از ویژگی‌های قابل توجه این تکنیک مقاومت قابل توجه آن در برابر پدیده چند مسیری است. در این

تکنیک از کانال های متعددی (۷۹ کانال) با پهنای باند نسبتاً کوچک استفاده شده و فرستنده و گیرنده به تناوب کانال فرکانسی خود را تغییر می‌دهند. این تغییر کانال هر ٤۰۰ میلی ثانیه بروز می‌کند لذا مشکل چند مسیری به شکل قابل ملاحظه‌ای منتفی می‌شود. زیرا گیرنده، سیگنال اصلی (که سریع‌تر از سایرین رسیده و عاری از تداخل است) را دریافت کرده و کانال فرکانسی خود را عوض می‌کند و سیگنال‌های انعکاسی زمانی به گیرنده می‌رسد که گیرنده کانال فرکانسی قبلی خود را عوض کرده و در نتیجه توسط گیرنده احساس و دریافت نمی‌شوند.



شکل۳-۱- پدیده چند مسیری

۸۰۲,۱۱a

۸۰۲,۱۱ aنسخه بعدی استانداردb۸۰۲,۱۱ بود . اولین محصولات مبتنی بر استاندارد a۸۰۲,۱۱ اوایل سال ۲۰۰۱ به بازار راه یافتند .

با وجود استفاده از فرکانس ٥GHz و همچنین سرعتی در حدود ٥٤Mbps استقبال چندانی از آ نها نشد . می توان دلایل اصلی این عدم استقبال را عدم سازگاری با b۸۰۲,۱۱ ، برد پایین ، هزینه بالا ،و همچنین استفاده از با ند فرکانسی نیازمند به مجوز نام برد .

استاندارد a۸۰۲,۱۱، از باند رادیویی جدیدی برای شبکه‌های محلی بی‌سیم استفاده می‌کند و پهنای باند شبکه‌های بی‌سیم را تا ٥٤ Mbps افزایش می‌دهد. این افزایش قابل توجه در پهنای باند مدیون تکنیک مدولاسیونی موسوم به OFDM است. نرخ‌های ارسال داده در استاندارد a۸۰۲,۱۱ IEEE عبارتند از:٥٤،٤٨،٣٦،٢٤،١٨،١٢،٩،٦ Mbps که بر اساس استاندارد، پشتیبانی از سرعت های ٦،١٢،٢٤ مگابیت در ثانیه اجباری است. برخی از کارشناسان شبکه‌های محلی بی‌سیم، استاندارد a۸۰۲,۱۱ IEEEرا نسل آینده ۸۰۲,۱۱ IEEEتلقی می‌کنند و حتی برخی از محصولات مانند تراشه‌های Atheros وکارت‌های شبکه PCMCIA/Cardbus محصول Access Inc Card. استاندارد

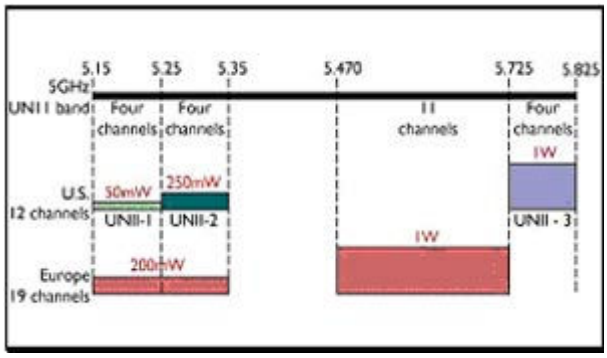
IEEE ۸۰۲,۱۱a را پیاده‌سازی کرده‌اند. بدون شک این پهنای باند وسیع و نرخ داده سریع محدودیت‌هایی را نیز به همراه دارد. در واقع افزایش پهنای باند در استاندارد IEEE ۸۰۲,۱۱a باعث شده است که محدوده عملیاتی آن در مقایسه با IEEE ۸۰۲,۱۱/b کاهش یابد. علاوه بر آن به سبب افزایش سربارهای پردازشی در پروتکل، تداخل، و تصحیح خطاها، پهنای باند واقعی به مراتب کمتر از پهنای باند اسمی این استاندارد است. همچنین در بسیاری از کاربردها امکان سنجی و حتی نصب تجهیزات اضافی نیز مورد نیاز است که به تبع آن موجب افزایش قیمتِ زیرساختارِ شبکه بی‌سیم می‌شود. زیرا محدوده عملیاتی در این استاندارد کمتر از محدوده عملیاتی در استاندارد IEEE ۸۰۲,۱۱b بوده و به همین خاطر به نقاط دسترسی یا ایستگاه پایه بیشتری نیاز خواهیم داشت که افزایش هزینه زیرساختار را به دنبال دارد. این استاندارد از باند فرکانسی خاصی موسوم به UNII استفاده می‌کند. این باند فرکانسی به سه قطعه پیوسته فرکانسی به شرح زیر تقسیم می‌شود:

UNII-۱ @ ۵,۲ GHz

UNII-۲ @ ۵,۷ GHz

UNII-۳ @ ۵,۸ GHz

یکی از تصورات غلط در زمینهاستانداردهای ۸۰۲,۱۱ این باور است که ۸۰۲,۱۱a قبل از ۸۰۲,۱۱b مورد بهره برداری واقع شده است. در حقیقت ۸۰۲,۱۱b نسل دوم استانداردهای بی‌سیم (پس از ۸۰۲,۱۱)است و ۸۰۲,۱۱a نسل سوم از این مجموعه استاندارد به شمار می‌رود. استاندارد ۸۰۲,۱۱a برخلاف ادعای بسیاری از فروشندگان تجهیزات بی‌سیم نمی‌تواند جایگزین ۸۰۲,۱۱b شود زیرا لایه فیزیکی مورد استفاده در هریک تفاوت اساسی با دیگری دارد. از سوی دیگر گذردهی (نرخ ارسال داده) و فواصل در هریک متفاوت است.



شکل٤-١- تخصیص باند فرکانسی در UNII

در شکل ٤-١ این سه ناحیه عملیاتی UNII و نیز توان مجاز تشعشع رادیویی از سوی FCC ملاحظه می‌شود. این سه ناحیه کاری ١٢ کانال فرکانسی را فراهم می‌کنند. باند ١-UNII برای کاربردهای فضای بسته، باند ٢-UNII برای کاربردهای فضای بسته و باز، و باند ٣-UNII برای کاربردهای فضای باز و پل بین شبکه‌ای به کار برده می‌شوند. این نواحی فرکانسی در ژاپن نیز قابل استفاده هستند. این استاندارد در حال حاضر در قارهاروپا قابل استفاده نیست. در اروپا HyperLAN٢برای شبکه‌های بی‌سیم مورد استفاده قرار می‌گیرد که به طور مشابه از باند فرکانسی ٨٠٢,١١aاستفاده می‌کند. یکی از نکات جالب توجه در استاندارد ٨٠٢,١١a تعریف کاربردهای پل سازی شبکه‌ای در کاربردهای داخلی و فضای باز است. در واقع این استاندارد مقررات لازم برای پل سازی و ارتباط بین شبکه‌ای از طریق پل را در کاربردهای داخلی و فضای باز فراهم می‌نماید. در یکی تقسیم بندی کلی می‌توان ویژگی ها و مزایای ٨٠٢,١١a را در سه محور زیر خلاصه نمود.

- افزایش در پهنای باند در مقایسه با استاندارد ٨٠٢,١١b (در استاندارد ٨٠٢,١١a حداکثر پهنای باند ٥٤ Mbps) می‌باشد.
- استفاده از طیف فرکانسی خلوت (باند فرکانسی ٥ GHz)
- استفاده از ١٢ کانال فرکانسی غیرپوشا (سه محدودهفرکانسی که در هریک ٤ کانال غیرپوشا وجود دارد)

افزایش پهنای باند

استاندارد ۸۰۲,۱۱a در مقایسه بـا ۸۰۲,۱۱b و پهنـای بانـد ۱۱ Mbps حـداکر پهنـای بانـد ٥٤ Mbps را فـراهم می‌کند. مهم‌ترین عامل افزایش قابل توجه پهنای بانـد در ایـن اسـتاندارد اسـتفاده از تکنیـک پیـشرفته مدولاسـیون، موسوم به OFDM است. تکنیکOFDM یک تکنولوژی (فنّاوری) تکامل یافته و بالغ در کاربردهای بـی‌سـیم بـه شمار می‌رود. این تکنولوژی مقاومت قابل توجهی در برابر تداخل رادیویی داشـته و تـأثیر کمتـری از پدیـده چنـد مسیری می‌پذیرد. OFDM تحت عناوین مدولاسیون چند حاملی و یا مدولاسیون چندآهنگی گسـسته نیـز شـناخته می‌شود. این تکنیک مدولاسیون علاوه بر شبکه‌های بی‌سیم در تلویزیون‌های دیجیتال (در اروپا، ژاپن، و اسـترالیا) و نیز به عنوان تکنولوژی پایه در خطوط مخابراتی ADSL مورد استفاده قرار می‌گیرد.

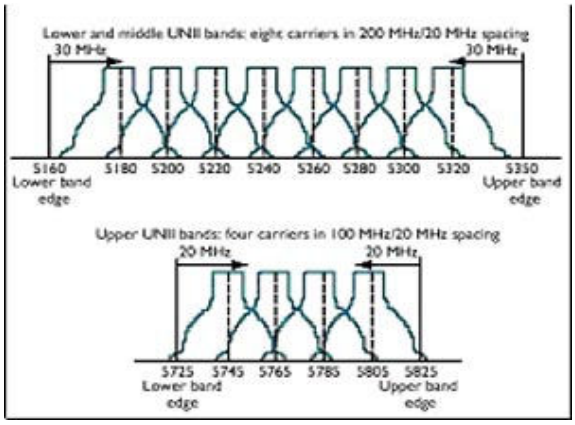
تکنیک OFDM از روش QAM و پردازش سیگنال‌های دیجیتال استفاده کرده و سـیگنال داده را بـا فرکـانس‌هـای دقیق و مشخصی تسهیم می‌کند. این فرکانس‌ها به گونه ای انتخاب می‌شوند که خاصیت تعامد را فراهم کننـد و بـه این ترتیب علیرغم همپوشانی فرکانسی هر یک از فرکانس های حامل به تنهایی آشکار می‌شـوند و نیـازی بـه بانـد محافظت برای فاصله گذاری بین فرکانس‌ها نیست. برای کسب اطلاعات بیشتر در خصوص این تکنیک مـی‌توانیـد به نشانی زیر مراجعه نمایید:

http://wireless.per.nl/telelearn/ofdm

در کنار افزایش پهنای باند در این استاندارد فواصل مورد استفاده نیز کاهش می‌یابند. در واقع باند فرکانسی ٥ GHz تقریباً دوبرابر باند فرکانسی ٢,٤ GHzاست که در استانداردa۸۰۲,۱۱ مورد استفاده قرار می‌گیرد. محدوده موثر در این استاندارد با توجه به سازندگان تراشه‌های بی‌سیم متفاوت و متغیر است ولی بـه عنـوان یـک قاعـده سرراسـت می‌توان فواصل در این

طیف فرکانسی تمیزتر

طیف فرکانسی UNII در مقایسه با طیف ISM خلوت‌تر است و کاربرد دیگری برای طیف UNII به جز شبکه‌های بی‌سیم تعریف و تخصیص داده نشده است. در حالی که در طیف فرکانسی ISM تجهیزات بی‌سیم متعددی نظیر تجهیزات پزشکی، اجاق های مایکروویو، تلفن‌های بی‌سیم و نظایر آن وجود دارند. این تجهیزات بی‌سیم در باند ۲,٤ GHz یا طیف ISM هیچگونه تداخلی با تجهیزات باند UNII (تجهیزات بی‌سیم a۸۰۲,۱۱) ندارند. شکل٤-۲ فرکانس مرکزی و فاصله‌های فرکانسی در باند UNII را نشان می‌دهد.



شکل٤-۲- فرکانس مرکزی و فواصل فرکانسی در باند UNII

کانال‌های غیرپوشا

باند فرکانسی UNII ، دوازده کانال منفرد و غیر پوشای فرکانسی را برای شبکه سازی فراهم می‌کند. از این ۱۲ کانال ۸ کانال مشخص (۲ , ۱-UNII) در شبکه‌های محلی بی‌سیم مورد استفاده قرار می‌گیرند. این ویژگی غیرپوشایی گسترش و پیاده سازی شبکه‌های بی‌سیم را ساده‌تر از باند ISM می‌کند که در آن تنها ۳ کانال غیر پوشا از مجموع ۱۱ کانال وجود دارد.

۸۰۲,۱۱g

۸۰۲,۱۱ gتلفیقی از هر دو مورد قبل است . استاندارد نوظهور شبکه های بی سیم که نیازهای پهنای باند ، سرعت وهزینه کاربران را بر آورده کرده در عین حال با استاندارد Wi-Fi نیز سازگاری دارد .

این استاندارد مشابه IEEE ۸۰۲,۱۱b از باند فرکانسی ۲,٤ GHz (یا طیف ISM) استفاده می‌کند و از تکنیک OFDM به عنوان روش مدولاسیون بهره می‌برد. البته PBCC نیز یکی از روش‌های جایگزین و تحت بررسی برای انتخاب تکنیک مدولاسیون در این استاندارد به شمار می‌رود. ۸۰۲,۱۱g از نظر فرکانسی، تعداد کانال های غیرپوشا، و توان مشابه ۸۰۲,۱۱b است. محدوده‌های عملیاتی نیز کم و بیش مشابه هستند با این تفاوت که حساسیت OFDM به نویز تاحدودی این محدوده عملیاتی را کاهش می‌دهد. پهنای باند ٥٤ Mbps یکی از اهداف احتمالی این استاندارد جدید به شمار می‌رود. یکی دیگر از مزایای جالب توجه ۸۰۲,۱۱g سازگاری با ۸۰۲,۱۱b است. در نتیجه ارتقاء از تجهیزات ۸۰۲,۱۱b به استاندارد جدید ۸۰۲,۱۱g امری سرراست خواهد بود. جدول٦-۱ – مقایسه استانداردهای بی‌سیم ۸۰۲,۱۱ IEEE

کارایی و مشخصات استاندارد ۸۰۲,۱۱g

نرخ انتقال داده ،برد ومسافت اتصال وسازگاری مشخصاتی هستند که در بین سه استاندارد تفاوت می کنند . این تفاوتها و تمایزات ناشی از مشخصاتی از قبیل فرکانس، مدولاسیون و تعداد نرخ داده می با شد .

نرخ انتقال داده در ۸۰۲,۱۱g

فن آوری ۸۰۲,۱۱g نرخ های انتقال داده متفاوتی را پشتیبانی می کند تا به کاربران امکان برقراری ارتباط در بهترین سرعت را بدهد .انتخاب بهترین نرخ انتقال داده موازنه–ای بین بدست آوردن بهترین نرخ انتقال و کمینه کردن تعداد خطا های رخ داده است .

هرگاه خطایی رخ دهد سیستم موظف به صرف زمان برای انتقال مجدد اطلاعات برای رفع خطای رخ داده است و این مسئله باعث می شود تا تعداد خطاهای رخ داده عاملی تعیین کننده باشد.

برد ومسافت در ۸۰۲,۱۱g

با افزایش فاصله از نقاط دسترسی (Access Point) تجهیزات مبتنی بر ۸۰۲,۱۱g نرخ انتقال را کاهش داده تا ارتباط با کاربران را حفظ کنند .

۸۰۲,۱۱g نیز مانند ۸۰۲,۱۱b دارای خصوصیات انتشار امواج رادیویی مشابه ای است زیرا مخابره سیگنالهای هر دو استاندارد در باند فرکانسی منحصر به فرد ۲,٤ GHz انجام می شود و به دلیل پیاده سازی یکسان این وضعیت

در این دو استاندارد خواص یکسان نرخ انتقال وماکسیمم برد مشاهده میشود .در حالیکه استاندارد a۸۰۲,۱۱ از باند فرکانسی کاملا مجزای GHzه استفاده میکند و قابلیت سازگاری با دو نوع دیگر را ندارد .

معمولا برد مسافتی دو نوع aوb (به دلیل استفاده از باند فرکانسی Ghz۲,٤)یکسان میباشد. استاندارد b۸۰۲,۱۱ از مدولاسیون CCK استفاده مـی کنـد در حالیکـه g۸۰۲,۱۱ هـم از مدولاسـیون CCK (بـرای حفـظ سـازگاری بـه b۸۰۲,۱۱)و هم از مدولاسیون OFDMبرای دستیابی به برد بیشتر بهره می جوید. a۸۰۲,۱۱هم از OFDM استفاده میکند اما درصد اعوجاج و خرابی سیگنا لها به دلیل استفاده از فرکانس بالاتر(امواج با فرکانس بالا از اجـسام عبـور می کنند) بیشتر است.

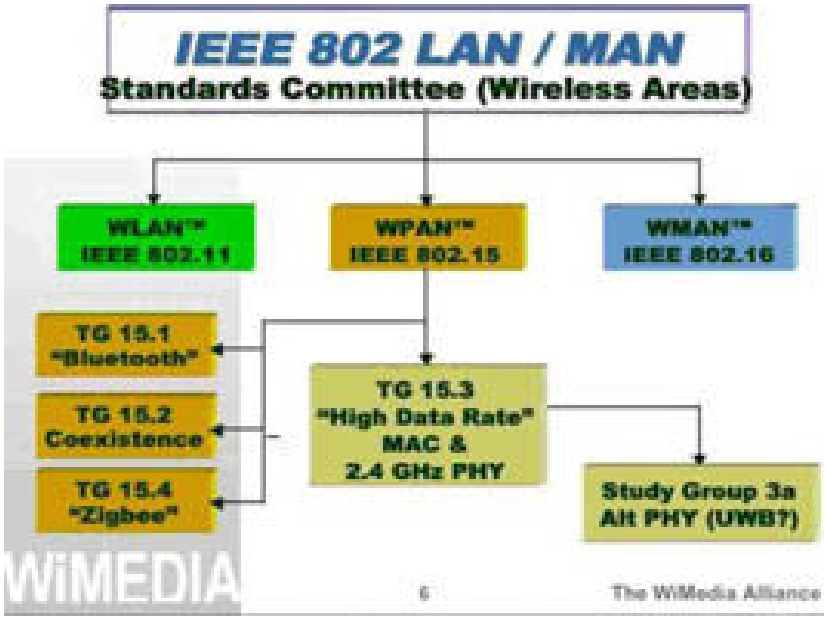
. تمام استانداردهای این خانواده بر اساس استاندارد های ذیل در لایه فیزیکی طراحی و پیاده سازی شده است.

- Ethernet
- CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)

جدول زیرسه استاندارد شبکه‌های بی‌سیم را با یکدیگر مقایسه می کند.

	IEEE ۸۰۲,۱۱b	IEEE ۸۰۲,۱۱a	IEEE ۸۰۲,۱۱g
کاربردهای احتمالی	- جایگزین شبکه‌های سیمی - فراهم آوردن تحرک و سیّار بودن کاربران - شبکه‌سازی در محل‌هایی که استفاده از سیم میسر نیست - پل‌سازی بین شبکه‌های محلی در فواصل دور (٤٠ کیلومتر)	- جایگزین شبکه‌های سیمی - فراهم کننده پهنای باند زیاد در کابردهای (صدا، تصویر، CAD و نظایر آن) - شبکه سازی در محل‌هایی که استفاده از سیم میسر نیست.	- ارتقاء شبکه‌های b۸۰۲,۱۱ و رقیبی برای a۸۰۲,۱۱ - کارایی مشابه با a۸۰۲,۱۱ در فواصل طولانی
مزایا	- استاندارد رایج و تکامل یافته - قیمت منطقی -گذردهی قابل قبول در فاصله زیاد (نرخ ارسال داده)	- گذردهی (نرخ ارسال داده) بالا در فواصل کم - افزایش تعداد کانال‌های فرکانسی غیرپوشا (٤ برابر بیشتر از b۸۰۲,۱۱) - تداخل فرکانسی کمتر	- سازگاری با b۸۰۲,۱۱ - محدوده عملیاتی زیاد (نظیر b۸۰۲,۱۱) - گذردهی (نرخ ارسال داده) بیشتر
معایب	- دارابودن کمترین گذردهی (نرخ ارسال داده) در مقایسه با سایر فناوری‌های بی‌سیم (۱۱ Mbps) - استفاده از تنها ۳ کانال فرکانسی غیر پوشا	- فنّاوری نسبتاً گران - ناسازگاری با b۸۰۲,۱۱ - محدوده عملیاتی کوچک - محدودیت‌های FCC برروی آنتن ها (حداکثر توان مجاز) در هر باند فرکانسی	- عدم وجود محصول فراگیر(احتمالاً تا اواسط سال۲۰۰۳ میلادی) - محدودیت‌ها کانال فرکانسی نظیر ۳۸۰۲,۱۱) b کانال غیرپوشا)

جدول زیر خلاصه سایر استانداردهای IEEE در شبکه های بی سیم را نمایش می دهد:



این مجموعه از استانداردها شامل سه استاندار می‌باشد که در شبکه‌های بی‌سیم مورد استفاده قرار می‌گیرد.

Best Usage	Modulation	Max. Data Transfer Rate	Frequency Range	IEEE
Outdoor	OFDM [۱]	٥٤ Mbps	٥.x GHz	٨٠٢,١١a
Indoor	PSK [۲] – CCK [۳]	١١ Mbps	٢,٤x GHz	٨٠٢,١١b
Indoor	OFDM	٥٤ Mbps	٢,٤x GHz	٨٠٢,١١g

۱. OFDM – Orthogonal Frequency Division Multiplexing

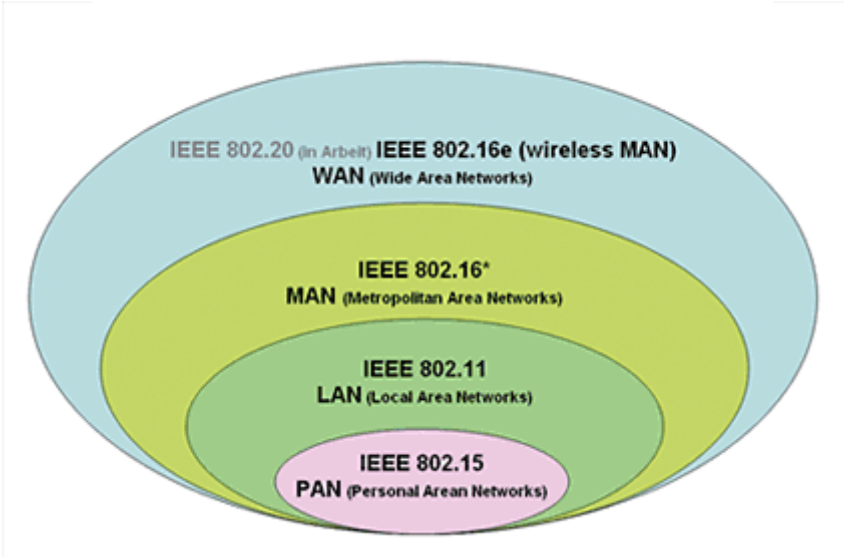
۲. PSK – Phase Shift Keying

۳. CCK – Complementary Code Keying

قابل ذکر است که استاندارد g دارای تطابق با استاندارد قدیمی b می‌باشد. بدین مفهوم که دستگاه‌های دارای استاندارد ٨٠٢,١١g قادر به کار با استاندارد قدیمی تر ٨٠٢,١١b می‌باشند.

استاندارد ۸۰۲ . ۱۱ e

این استاندارد برای تکمیل استانداردهای *a,b,g* با ویژگی امکان ایجاد اولویت در ارسال بسته‌های اطلاعات حساس به تاخیر زمانی مانند بسته های صوتی و تصویری *(Voice & Video Packet)* تعریف شده است. به این ترتیب با ایجاد اولویت در ارسال بسته‌های حاوی اطلاعات صوتی و تصویری کیفیت ارسال صوت و تصویر بالا رفته و تاخیر *(Latency)* در ارسال و دریافت بوجود نخواهد آمد.



کاربرد های wifi

تکنولوژی وای فای علاوه بر استفاده در ارتباط رایانه های شخصی در اتصال به اینترنت به صورت بی سیم امکان استفاده از هر شبکه دیگری رانیز دارد.به عنوان نمونه در تلفن همراه های نسل جدید امکان اتصال به اینترنت از طریق واب فای فراهم شده و نیز سرویس (roice)اتقال صدا از طریق تکنولوژی اینترنت که امکان بر قراری تماس تلفنی روی شبکه های رایانه ای را مقدور می سازد نیز از wifi بهره می گیرد.با استفاده از Telephony Dualmode و دستگاه های تلفن همراه نیز قادر خواهند بود با استفاده لز تکنولوژی وای فای تماس هایی با کیفیت تکنولوژی سلولی را بر قرار سازند و بدین ترتیب شما امکان اتصال به اینترنت روی گوشی خود را خواهید داشت و هم امکان مکالمه تلفنی را .

دلایل رشد wifi

شبکه های مبتنی بر wifi راه موفقیت و پیشرفت را در پیش گرفته است. تعداد کاربران wifiکه در سال۲۰۰۰درحدود۲/۵ ملیون نفر بود اکنون به ۱۸ ملیون کاربر رسیده است و می رود تا مسیر رشد و پیشرفت خود را ادامه دهد از مهمترین دلایل رشد wifi می توان به موارد زیر اشاره کرد:

۱)پشتیبان شرکت های مختلف:شرکت های بزرگ و معتبری همچون مایکروسافت ، اینتل سیسکو وای بی ام به شدت مشغول کار بر روی تکنولوژی wifi هستند و سرمایه گذاری های هنگفتی نیز در این زمینه انجام داده اند به عنوان نمونه شرکت اینتل سیصد ملیون دلار برای توسعه wifi بر روی centrino سرمایه گذاری کرده است.

۲)توسعه ارتباط باند پهن:استفاده از فناوری wifi سبب توسعه شبکه های باند پهن شده است به گونه ای که در سال جاری در حدود ۳۰ درصد رشددر زمینه باند پهن مشاهده شده است.

۳)شبکه های بزرگ ملی:هم اکنون در برخی از کشور های دنیا شبکه بزرگ ملی wifi در حال فعالیت است به عنوان نمونه در کشور آمریکا چهار شبکهBoingo،comeate Network، voice stream،Toshiba مشغول سرویس دهی به کاربران هستند.

٤)تجهیزات آماده:شرکت های تولید کننده سخت افزار در سال های اخیر همراه با سخت افزارهای خود لوازم و متعلقات مورد نیاز سیستم های wifi را به صورت آماده در اختیار مشتریان قرار می دهندو دیگر نیازی به تهیه این وسایل از بازارها رایانه به صورت جداگانه وجود ندارد.هم اکنون شرکت های Dell،Toshiba،..... درراینه ها و قطعات تولیدی خود تکنولوژی wifiرا گنجانده اند .بر طبق اعلام شرکت های سخت افزاری در دو سال آینده همه رایانه های همراه(laptop)به تجهیزات wifi مجهز خواهند شد.

۵)گسترش شبکه:پیشگامان صنعت wifi در همه نقاط دنیا به شدت در حال توسعه شبکه های wifi هستند به عنوان نمونه در همه پارکها،رستوران ها و اماکن تفریحی این تکنولوژی ها به چشم می خورد.

٦)نو آوری های بیشتر:تکنولوژی wifi به دلیل تازه واردبودن به سرعت در حال پیشرفت است.شرکت های اینتل وMash در حال ساختن آنتن هایی هستندکه نسبت به آنتن های فعلی محدوده بیشتری راپوشش می دهدبه علاوه شرکت های سازنده گوشی تلفن همراه نیز در حال ساخت گوشی هایی با امکانات wifi هستند.

نقاط ضغف wifi

۱)قیمت های گران:هزینه های اشتراک ماهانه در بسیاری از کشور ها در حدود ۵۰ دلار در ماه است.

۲)هزینه های پنهان فراوان: جدا از هزینه های اولیه wifi شما بایدهزینه های پنهان دیگری نیز مانند نصب و نگداری تجهیزات شبکه و نیز راه حل امنیتی را بپردازد.

۳)فواصل کوتاه: هم اکنون فاصله ای را که به جرات اعلام کرد در حدود یک صد متر است که با وجود موانع فیزیکی موجود در ساختمان ها و ادارات این فاصله دریافت سیگنال کمتر نیز خواهد شد.

٤)عدم پوشش همه نقاط:در برخی کشور ها که تکنولوژی wifi فعال شدهپوشش کابل شبکه فراهم نشدهو شما مجبور به استفاده از سرویس دهندگان مختلف در نقاط جغرافیایی متفاوت خواهید بود.

۵)مشخص نبودن استانداردها:استانداردهای شربت های ارائه دهنده تجهیزات وای فای استفاده از طیف رادیویی بدون مجوز را ترجیح می دهند زیرا در این صورت هزینه های ان کاهش خواهد یافت و همین امر سبب شد که استاندارد واحدی برای این کار طراحی نشود اما در سال های اخیر سازندگان به سمت متحد شدن استانداردها حرکت رو به جلویی را آغاز کردند.

٦)عدم وجود امنیت:در شبکه های بی سیم قبلی اجازه ارتباط کاربران غیر مجاز شبکه نیز داده می شدکه امکان شنود از طریق این کاربران یکی از خطرات این قبیل از شبکه ها بود اما هم اکنون سازندگان به سوی توسعه شبکه های امن حرکت خود را آغاز کردند.

۳– امنیت شبکه های بی سیم

۳-۱امنیت شبکه بی سیم

۳-۲چهار مشکل امنیتی مهم شبکه های بی سیم ۸۰۲,۱۱

۳-۳سرویس امنیتی استاندارد ۸۰۲,۱۱

۳-٤ قابلیت‌ها و ابعاد امنیتی استاندارد ۸۰۲,۱۱

مقدمه

در طی چند سال گذشته یک پیام واضح و روشن وجود داشت ایجاد امنیت برای تکنولوژی wifi در عین سودمندی بسیار آن کار ساده ای نیست در اکثر نقاط دسترسی بی سیم سیتم امنیتی به طور پیش فرض غیر فعال است و حتی سیستم ایمنی موجود در آن ها نیز مناسب و کافی نیست (wep(wired equivalent privacy اولین کوشش برای ایمن کردن wifi مکرا نقاط ضعف زیادی را به نمایش گذاشته است .ابزار بسیلر زیادی برای حمله به wifi وجود دارد که این ابزار فقط در عرض چند دقیقه می توانند کلید به کار رفته برای محافظت از شبکه را دور بزنند و از کار بیندازند.حتی نسل بعدی تکنیک های ایمنی هنوز هم مشکلات متعددی دارند جدیدترین مشخصات ایمنی بی سیم یعنی ۸۰۲,۱۱ امکان انجام انواع روش های تایید اعتبار شبکه شامل کلمه های عبور ساده و سایر مکانیزم های تائید اعتبار ضعیف را که پشت سر گذاشتن آنها بسیار ساده است فراهم می کند. با رواج بیشتر استفاده از اینترنت بی‌سیم، کاهش قیمت آن و افزایش سهولت دسترسی به آن طبعاً مشکلات امنیتی آن نیز افزایش می‌یابد. از جمله مشکلات امنیتی در زمینهٔ WiFi می‌توان به موارد زیر اشاره کرد:

امنیت شبکه بی سیم

Rouge Access Point Problem:

این مشکل یکی از مهم‌ترین نگرانی‌های امنیتی در زمینهٔ استفاده از شبکه‌های WiFi به حساب می‌آید. Rouge Access Point به هر نقطهٔ دسترسی(WiFi (Access Point اطلاق می‌شود که بدون اجازهٔ شما به شبکه وصل شده است و از امکانات آن از جمله پهنای باند اینترنت استفاده می‌کند.این معزل علاوه بر اتصال غیر مجاز به شبکه و استفاده از پهنای باند آن سایر مشکلات امنیتی مانند hacking را نیز سبب شود.

- دستگاه‌های ناامن WiFi: از جمله Access Pointها و دستگاه‌های مورد استفادهٔ کاربران ممکن است موجب مشکلات جدی در این زمینه گردد. و این مورد معمولاً بیش از همه مورد توجه هکرهاست.
- تنظیمات ناصحیح دستگاه‌های بی‌سیم و عدم تغییر در تنظیمات پیش‌فرض آن‌ها امکانات متنوع نفوذگران

استاندارد ۸۰۲,۱۱ سرویس‌های مجزا و مشخصی را برای تأمین یک محیط امن بی‌سیم در اختیار قرار می‌دهد. این سرویس‌ها اغلب توسط پروتکل WEP (Wired Equivalent Privacy) تأمین می‌گردند و وظیفه‌ی آن‌ها امن‌سازی ارتباط میان مخدوم‌ها و نقاط دسترسی بی‌سیم است. درک لایه‌یی که این پروتکل به امن‌سازی آن می‌پردازد اهمیت ویژه‌یی دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه‌های دیگر، غیر از لایه‌ی ارتباطی بی‌سیم که مبتنی بر استاندارد ۸۰۲,۱۱ است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه‌ی بی‌سیم به‌معنی استفاده از قابلیت درونی استاندارد شبکه‌های محلی بی‌سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.

با به کار گیری تائید اعتبار دو طرفه مبتنی بر مجوز با رمزگذاری مبتنی بر AES شبکه های wifi مدرن می توانند حتی برای مهاجمان حرفه ای نیز یک مانع قابل توجه محسوب شوند .با بعضی از wap کاربران می توانند عدم پخش SSIDرا انتخاب کنند.SSID سر واژه عبارت زیر است:SSID service set identifier ورود نفوذ گران به شبکه را دشوارتر می سازد.

شبکه‌های Wi-Fi دارای امکانات امنیتی بسیار قدرتمند می‌باشند که از دسترسی غیر مجاز به این شبکه‌ها جلوگیری می‌کند. از جمله این استانداردها می‌توان به

۱. IEEE ۸۰۲,۱x
۲. WEP - Wired Equivalent Privacy
۳. WPA - Wi-Fi Protected Access
٤. TKIP - Temporal Key Integrity Protocol

اشاره کرد. علاوه بر استانداردهای یاد شده در Access Point هایی که دارای نرم افزارهای کارآمد می‌باشند، امکان فیلتر کردن MAC Address وجود دارد، در این صورت فقط MAC Address های تعریف شده در نرم افزار AP امکان بهره برداری از سرویس AP را دارا می‌باشند.

Hotspot های وای فای می توانند آشکار و باز باشند یا محفوظ باشند .اگر آنها آشکار باشند هر کسی با یک کارت وای فای می تواند به hotspot دسترسی داشته باشد اما اگر محفوظ باشد لازم است کاربر رمز wep را

برای اتصال بداند . WEP یک سیستم رمزگذاری داده ها است که۸۰۲/۱۱ از طریق هوا ارسال می کند . WEP دو نوع دارد : رمز گذلری ٦٤ بیتی و رمز گذلری ۱۲۸ بیتی . رمزگذلری ۱۲۸ بیتی امن تر است و افراد بیشتر ازان استفاده می کنند غیر قابل دسترس است مگر اینکه کد WEP را بداند.

اگر شما یک hotspot در منزل خود نصب کنید با ایجاد و استفاده از یک کد wep می توانید از استراق سمع تصادفی شبکه تان توسط همسایگان خود جلوگیری کنید .چه در خانه و چه در بیرون شما باید کد wep را بدانید سپس ان را در نرم افزار کارت وای فتی وارد کنید تا بتوانید به شبکه دسترسی داشته باشید.

با به کارگیری نکات زیر می توان یک امنیت شبکه بی سیم را تا حد قابل قبولی بهبود بخشید.

لازم به ذکر است که این نکات لازم است ولی کافی نیست.

۱. کلمه عبور پیش‌فرض مدیر سیستم(administrator) را روی نقاط دسترسی و مسیریاب‌های بی‌سیم تغییر دهید.

اغلب نقاط دسترسی (Access Point)و مسیریاب‌های بی‌سیم امکان مدیریت شبکه WiFi را از طریق یک حساب کاربری مدیریتی فراهم می‌کنند. این حساب کاربری امکان دسترسی ابزار و پیکربندی آن را با نام کاربری و کلمه عبور فراهم می‌کند. اغلب تولیدکنندگان نام کاربری و کلمه عبور را در کارخانه تنظیم می‌کنند . نام کاربری معمول admin یا administrator و کلمه عبور یا خالی است یا کلماتی مثل admin، public، password و .... می‌باشد.

اولین گام برای افزایش امنیت شبکه بی‌سیم تغییر کلمه عبور پیش‌فرض نقاط دسترسی و مسیریاب‌های بی‌سیم بلافاصله پس از نصب است. اغلب ابزارها اجازه تغییر نام کاربری را نمی‌دهند اما اگر ابزارهای شما این امکان را می‌دهند، اکیدا توصیه می‌شود که نام کاربری را هم تغییر دهید.

برای امن نگه‌داشتن شبکه در آینده، می‌بایست به‌طور منظم این کلمه عبور را تغییر دهید. اغلب کارشناسان توصیه می‌کنند کلمه عبور را بعد از ۳۰ تا ۹۰ روز تغییر دهید.

۲. فعال‌سازی قابلیت WPA/WEP

WPA (WiFi Protected Access) یک استاندارد امنیتی برای شبکه‌های بی‌سیم است (با Windows XP Product Activation اشتباه نشود). برای استفاده از WPA با Windows XP باید Clientهای دارای Windows XP را به صورت دستی patch کنید و هم‌چنین مطمئن شوید کارت شبکه‌ها و نقاط دسترسی به درستی پیکربندی شده‌اند.

برای پیکربندی WPA در شبکه با clientهای دارای ویندوز XP مراحل زیر را انجام دهید:

۱. نوشتار Overview of the WPA wireless security update in Windows XP را مطالعه کنید.
۲. بررسی کنید که تمام Client ها حداقل Service Pack۱ داشته باشند.
۳. روی هر Client بررسی کنید که کارت شبکه با سرویس WZC(Windows Zero Configuration) سازگار باشد.
٤. برای هر client وصله Windows XP Support Patch for Wi-Fi Protected Access را بارگزاری و نصب کنید.
۵. تغییرات لازم برای نقاط دسترسی بی‌سیم از گام ۱ را اعمال کنید.
٦. تغییرات لازم برای کارت شبکه‌های بی‌سیم از گام ۱ را اعمال کنید.

۳. تغییر SSID پیش فرض

نقاط دسترسی و مسیریاب‌های بی‌سیم دارای یک نام شبکه SSID(Service Set Identifier) هستند که توسط تولیدکنندگان به‌طور پیش‌فرض انتخاب می‌شود. SSID از ابزارهای پیکربندی بر مبنای وب یا ویندوز این سازندگان قابل دسترسی است. اغلب SSIDهای پیش فرض کلمات ساده‌ای مثل wireless، netgear، linksys، default و ... هستند. هرچند نفوذگر صرفا با دانستن SSID قادر به نفوذ به شبکه شما نیست ولی این مساله به عنوان یک نقطه شروع خوب برای نفوذگر به حساب می آید. زمانی که کسی شبکه ای با SSID پیش فرض بیابد، با دانستن این نکته که به احتمال فراوان این شبکه به درستی پیکربندی نشده است، ترغیب به نفوذ به شبکه می‌شود.

SSID می تواند هر زمانی تغییر کند به شرطی که این تغییر در تمام clientها نیز اعمال شود. برای افزایش امنیت شبکه های بی سیم، نام پیش فرض SSID را تغییر دهید. در انتخاب SSID توصیه های زیر را در نظر داشته باشید:

- از نام، آدرس، تاریخ تولد، شماره تلفن یا دیگر اطلاعات شخصی تان به عنوان بخشی از SSID استفاده نکنید.
- از کلمات عبور نام کاربری ویندوزتان یا emailتان یا ... استفاده نکنید.
- با استفاده از عباراتی مثل "TOP_SECRET"، "FUNNY_BOX" و ... نفوذگران را وسوسه نکنید.!!!
- از ترکیب حروف و اعداد استفاده کنید.
- عباراتی با طول حداکثر یا نزدیک به حداکثر انتخاب کنید.
- هرچند ماه یک بار SSIDتان را تغییر دهید.

۴. قابلیت پالایش آدرس MAC را روی نقاط دسترسی و مسیریاب‌های بی‌سیم فعال کنید.

اغلب نقاط دسترسی و مسیریاب های بی سیم دارای قابلیتی به نام پالایش آدرس MAC (MAC Address Filtering) هستند. این مشخصه اغلب به‌طور پیش فرض فعال نیست. برای افزایش امنیت شبکه بی سیم تان این قابلیت را فعال کنید. در صورتی که این قابلیت فعال نباشد، هر clientای با دانستن SSID شبکه شما (در نظر داشته باشید که فهمیدن SSID کار بسیار ساده ای است) شاید چند پارامتر امنیتی دیگر مثل کلید رمزگذاری (در صورتی که قابلیت WEP فعال باشد) می تواند به شبکه شما وصل شود.

برای تنظیم قابلیت پالایش آدرس MAC شما به عنوان مدیر شبکه بی سیم باید لیست clientهایی که مجازند به شبکه وصل شوند را پیکربندی کنید. ابتدا آدرس MAC هر client را از طریق سیستم عامل یا ابزارهای پیکربندی به دست آورید و سپس آن ها را در صفحه پیکربندی نقاط دسترسی و مسیریاب های بی سیم وارد کنید و نهایتا قابلیت پالایش را فعال کنید. از این پس هر درخواست اتصال به شبکه بی سیم که برسد آدرس MAC آن با لیست تنظیم شده بررسی شده و در صورتی که در لیست نباشد اجازه اتصال به شبکه را نمی یابد. البته باید نوجه داشت که نفوذگران با جعل آدرس MAC (MAC Spoofing) قادرند به شبکه بی سیم شما وصل شوند ولی این مساله نباید باعث شود که شما از خیر این قابلیت بگذرید.

۵. قابلیت همه‌پخشی SSID را روی نقاط دسترسی و مسیریاب‌های بی‌سیم غیرفعال کنید.

اغلب نقاط دسترسی و مسیریاب های بی سیم به‌طور خودکار SSID خوشان را در فواصل زمانی مشخص پخش می کنند. این مشخصه برای این است که clientها بتوانند به‌طور پویا شبکه های بی سیم را تشخیص دهند و بین آن ها جابه‌جا شوند (از شبکه ای به شبکه دیگر نقل مکان کنند). لازم به ذکر است که این مشخصه برای hotspotهای تجاری و سیار طراحی شده است که clientهای زیادی می آیند و می روند ولی برای شبکه های خانگی لازم نیست. از آن جایی که SSID به صورت واضح پخش می شود و هیچ رمزگذاری روی آن صورت نمی گیرد، به دست آوردن آن توسط نفوذگران کار راحتی است. همان‌طور که در گام ۳ اشاره شد نفوذگر با دانستن SSID یک مرحله به هدف نزدیک تر می شود.

در یک شبکه بی سیم بحث roaming (جابه‌جایی بین دو شبکه بی سیم) مطرح نیست و پخش کردن SSID هیچ ضرورتی ندارد. برای افزایش امنیت شبکه بی سیم باید این قابلیت را غیرفعال کنید. یک بار که client شما با SSID درست پیکربندی شد دیگر نیازی به پیغام های همه‌پخشی نیست.

دقت داشته باشید که غیرفعال کردن قابلیت همه‌پخشی SSID فقط یکی از تکنیک‌های محکم‌سازی و افزایش امنیت شبکه‌های بی سیم است. این روش ۱۰۰ درصد موثر نیست و نفوذگرها هنوز می توانند با sniff کردن پیغام های مختلف پخش شده در پروتکل WiFi، SSID را تشخیص دهند. در واقع تکنیک هایی مثل غیرفعال کردن همه‌پخشی SSID باعث می شئد که شبکه بی سیم شما هدف راحتی برای نفوذگران نباشد.

اگر هم اکنون دارای یک شبکه بی سیم میباشید ممکن است این مسئله را در نظر بگیرید که آیا شبکه تان ایمن است یا خیر؟ چهار مورد وجود دارند که شما می توانید انجام دهید که اطمینان حاصل نمایید که شبکه تان امن میباشد .

۱- اطمینان حاصل نمایید که نقطه یا نقاط دسترسی SSID تان (شناسایی تنظیم کننده خدمات) را پخش نمی نماید (که بطور اساسی یک شناسایی کننده برای شبکه شما میباشد

۲- اطمینان حاصل نمایید که نقطه یا نقاط دسترسی تان ترافیک بی سیم را با بکارگیری WEP رمز سازی می نماید.

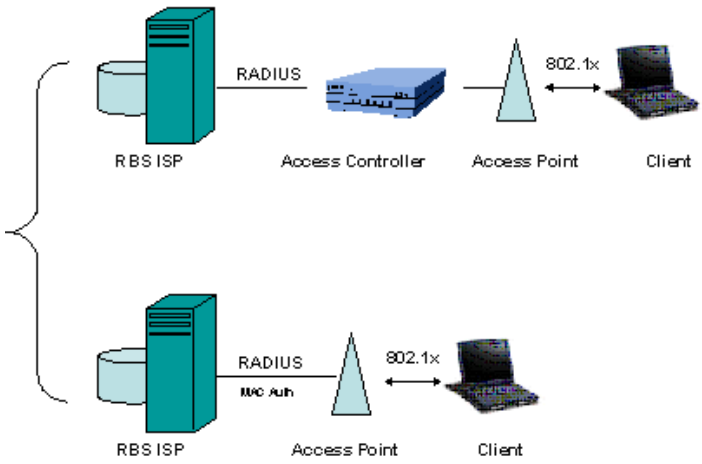
۳- یک سیستم "شناسایی بدون اجازه وارد شدن افراد غیر مجاز به شبکه بی سیم تان" را خریداری نمایید. تعداد زیادی از این محصولات که آماده و قابل دسترس میباشند، طراحی شده اند که بشما کمک نمایند که امنیت شبکهء WiFiتان و همینطور اینکه چه افرادی از آن استفاده می نمایند را دیده بانی نمایید.

٤- اگر نیاز به امنیت خیلی بالا دارید، می توانید یا اطمینان حاصل نمایید که افرادیکه با شبکه شما کار می نمایند بطور مناسب و کارآیی آموزش دیده و یا از یک مشاور بی سیم استفاده نمایید. شما نیاز خواهید داشت که نقاط دسترسی غیر استاندارد و اختصاصی از شرکتهایی مثل سیسکو (Cisco) خریداری نمایید (اگرچه حتی بعضی استانداردهای اختصاصی از شرکتهایی مثل (Cisco) مشکل خودشان را دارند). متاسفانه این بطور قابل ملاحظه ای هزینه شبکه بی سیم شما را افزایش خواهد داد.

چهار مشکل امنیتی مهم شبکه های بی سیم ۸۰۲.۱۱

موفقیت حیرت انگیز ۸۰۲,۱۱ به علت توسعه «اترنت بی سیم» است. همچنانکه ۸۰۲,۱۱ به ترقی خود ادامه می دهد، تفاوت هایش با اترنت بیشتر مشخص می شود. بیشتر این تفاوت ها به دلیل نا آشنایی نسبی بسیاری از مدیران شبکه با لایه فیزیکی فرکانس رادیویی است. در حالیکه همه مدیران شبکه باید درک پایه ای از لینک رادیویی داشته باشند، تعدادی از ابزارها برای کمک به آنها به خدمت گرفته می شوند. آنالایزرهای (تحلیل کننده) شبکه های بی سیم برای مدت ها ابزاری لازم برای مهندسان شبکه در اشکال زدایی و تحلیل پروتکل بوده اند. بسیاری از آنالایزرها بعضی کارکردهای امنیتی را نیز اضافه کرده اند که به آنها اجازه کار با عملکردهای بازرسی امنیتی را نیز می دهد.

در این سلسله چهار مشکل از مهم ترین آسیب پذیری های امنیتی موجود در LANهای بی سیم، راه حل آنها و در نهایت چگونگی ساخت یک شبکه بی سیم امن مورد بحث قرار می گیرد. بسیاری از پرسش ها در این زمینه در مورد ابزارهایی است که مدیران شبکه می توانند استفاده کنند. یک آنالایزر از اولین خریدهایی است که یک مدیر شبکه باید انجام دهد. آنالایزرها علاوه بر عملکردهای سنتی تحلیل پروتکل و ابزار تشخیص عیب، می توانند برای تشخیص بسیاری از نگرانی های امنیتی که استفاده از شبکه بی سیم را کند می کنند، استفاده شوند.



مسأله شماره ۱: دسترسی آسان

LANهای بی سیم به آسانی پیدا می شوند. برای فعال کردن کلاینت ها در هنگام یافتن آنها، شبکه ها باید فریم های Beacon با پارامتر های شبکه را ارسال کنند. البته، اطلاعات مورد نیاز برای پیوستن به یک شبکه، اطلاعاتی است که برای اقدام به یک حمله روی شبکه نیاز است. فریم های Beacon توسط هیچ فانکشن اختصاصی پردازش نمی شوند و این به این معنی است که شبکه ۸۰۲,۱۱ شما و پارامترهایش برای هر شخصی با یک کارت ۸۰۲,۱۱ قابل استفاده است. نفوذگران با آنتن های قوی می توانند شبکه ها را در مسیرها یا ساختمان های نزدیک بیابند و ممکن است اقدام به انجام حملاتی کنند حتی بدون اینکه به امکانات شما دسترسی فیزیکی داشته باشند.

راه حل شماره ۱: تقویت کنترل دسترسی قوی

دسترسی آسان الزاماً با آسیب پذیری مترادف نیست. شبکه های بی سیم برای ایجاد امکان اتصال مناسب طراحی شده اند، اما می توانند با اتخاذ سیاستهای امنیتی مناسب تا حد زیادی مقاوم شوند. یک شبکه بی سیم می تواند تا

حد زیادی در این اتاق محافظت شده از نظر الکترومغناطیس محدود شود که اجازه نشت سطوح بالایی از فرکانس رادیویی را نمی دهد. به هرحال، برای بیشتر موسسات چنین برد هایی لازم نیستند. تضمین اینکه شبکه های بی سیم تحت تأثیر کنترل دسترسی قوی هستند، می تواند از خطر سوءاستفاده از شبکه بی سیم بکاهد.

تضمین امنیت روی یک شبکه بی سیم تا حدی به عنوان بخشی از طراحی مطرح است. شبکه ها باید نقاط دسترسی را در بیرون ابزار پیرامونی امنیت مانند فایروال ها قرار دهند و مدیران شبکه باید به استفاده از VPNها برای میسر کردن دسترسی به شبکه توجه کنند. یک سیستم قوی تأیید هویت کاربر باید به کار گرفته شود و ترجیحاً با استفاده از محصولات جدید که برپایه استاندارد IEEE ۸۰۲,۱X هستند. ۸۰۲,۱X انواع فریم های جدید برای تأیید هویت کاربر را تعریف می کند و از دیتابیس های کاربری جامعی مانند RADIUS بهره می گیرد. آنالایزرهای باسیم سنتی می توانند با نگاه کردن به تقاضاهای RADIUS و پاسخ ها، امکان درک پروسه تأیید هویت را فراهم کنند. یک سیستم آنالیز خبره برای تأیید هویت ۸۰۲,۱۱ شامل یک روتین عیب یابی مشخص برای LANهاست که ترافیک تأیید هویت را نظاره می کند و امکان تشخیص عیب را برای مدیران شبکه فراهم می کند که به آنالیز بسیار دقیق و کدگشایی فریم احتیاج ندارد. سیستم های آنالیز خبره که پیام های تأیید هویت ۸۰۲,۱X را دنبال می کنند، ثابت کرده اند که برای استفاده در LANهای استفاده کننده از ۸۰۲,۱X فوق العاده باارزش هستند.

هرگونه طراحی، بدون در نظر گرفتن میزان قدرت آن، باید مرتباً بررسی شود تا سازگاری چینش فعلی را با اهداف امنیتی طراحی تضمین کند. بعضی موتورهای آنالیز تحلیل عمیقی روی فریم ها انجام می دهند و می توانند چندین مسأله معمول امنیت ۸۰۲,۱X را تشخیص دهند. تعدادی از حملات روی شبکه های باسیم در سال های گذشته شناخته شده اند و لذا وصله های فعلی به خوبی تمام ضعف های شناخته شده را در این گونه شبکه ها نشان می دهند. آنالایزرهای خبره پیاده سازی های ضعیف را برای مدیران شبکه مشخص می کنند و به این ترتیب مدیران شبکه می توانند با به کارگیری سخت افزار و نرم افزار ارتقاء یافته، امنیت شبکه را حفظ کنند.

پیکربندی های نامناسب ممکن است منبع عمده آسیب پذیری امنیتی باشد، مخصوصاً اگر LANهای بی سیم بدون نظارت مهندسان امنیتی به کارگرفته شده باشند. موتورهای آنالیز خبره می توانند زمانی را که پیکربندی های پیش فرض کارخانه مورد استفاده قرار می گیرند، شناسایی کنند و به این ترتیب می توانند به ناظران کمک کنند که نقاطی از دسترسی را که بمنظور استفاده از ویژگی های امنیتی پیکربندی نشده اند، تعیین موقعیت کنند. این آنالایزرها

همچنین می توانند هنگامی که وسایلی از ابزار امنیتی قوی مانند VPNها یا ۸۰۲,۱x استفاده نمی کنند، علائم هشدار دهنده را ثبت کنند.

مسأله شماره ۲: نقاط دسترسی نامطلوب

دسترسی آسان به شبکه های LAN بی سیم امری منفک از راه اندازی آسان آن نیست. این دو خصوصیت در هنگام ترکیب شدن با یکدیگر می توانند برای مدیران شبکه و مسوولان امنیتی ایجاد دردسر کنند. هر کاربر می تواند به فروشگاه کامپیوتر نزدیک خود برود، یک نقطه دسترسی! بخرد و بدون کسب اجازه ای خاص به کل شبکه متصل شود. بسیاری از نقاط دسترسی با اختیارات مدیران میانی عرضه می شوند و لذا دپارتمان ها ممکن است بتوانند LAN بی سیمشان را بدون صدور اجازه از یک سازمان IT مرکزی در معرض عموم قرار دهند. این دسترسی به اصطلاح «نامطلوب» بکارگرفته شده توسط کاربران ، خطرات امنیتی بزرگی را مطرح می کند. کاربران در زمینه امنیتی خبره نیستند و ممکن است از خطرات ایجاد شده توسط LAN های بی سیم آگاه نباشند. ثبت بسیاری از ورودها به شبکه نشان از آن دارد که ویژگی های امنیتی فعال نیستند و بخش بزرگی از آنها تغییراتی نسبت به پیکربندی پیش فرض نداشته اند و با همان پیکربندی راه اندازی شده اند.

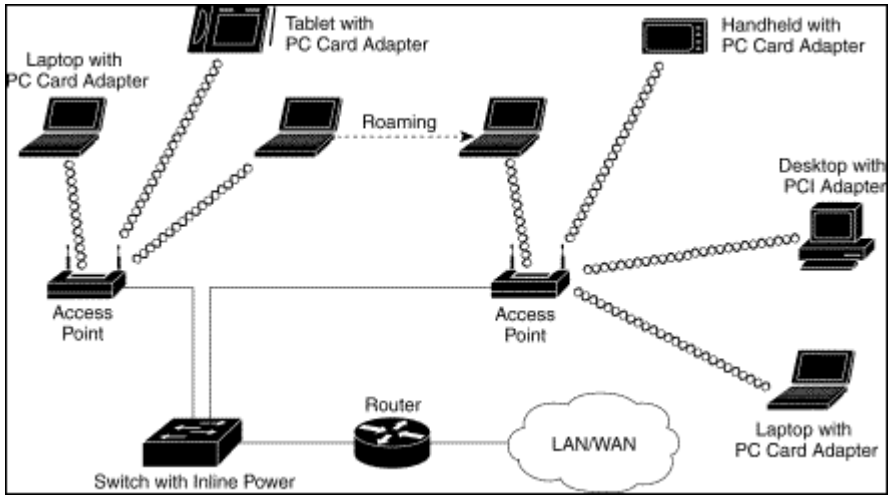
راه حل شماره۲ : رسیدگی های منظم به سایت

مانند هر تکنولوژی دیگر شبکه، شبکه های بی سیم به مراقبت از سوی مدیران امنیتی نیاز دارند. بسیاری از این تکنولوژی ها به دلیل سهولت استفاده مورد بهره برداری نادرست قرار می گیرند، لذا آموختن نحوه یافتن شبکه های امن نشده از اهمیت بالایی برخوردار است.

روش بدیهی یافتن این شبکه ها انجام همان کاری است که نفوذگران انجام می دهند: استفاده از یک آنتن و جستجوی آنها به این منظور که بتوانید قبل از نفوذگران این شبکه ها را پیدا کنید. نظارت های فیزیکی سایت باید

به صورت مرتب و در حد امکان انجام گیرد. اگرچه هرچه نظارت ها سریع تر انجام گیـرد، امکـان کـشف اسـتفاده های غیرمجاز بیشتر است، اما زمان زیادی که کارمندان مسوول این امر باید صرف کنند، کشف تمامی استفاده هـای غیرمجاز را بجز برای محیط های بسیار حساس، غیرقابل توجیه می کند. یک راهکار برای عدم امکان حـضور دائـم می تواند انتخاب ابزاری در اندازه دستی باشد. این عمل می تواند استفاده تکنسین ها از اسکنرهای دستی در هنگـام انجام امور پشتیبانی کاربران، برای کشف شبکه های غیرمجاز باشد.

یکی از بزرگترین تغییرات در بازار ۸۰۲,۱۱ در سال های اخیر ظهور ۸۰۲,۱۱a به عنوان یک محصول تجـاری قابـل دوام بود. این موفقیت نیاز به ارائـه ابزارهـایی بـرای مـدیران شـبکه هـای ۸۰۲,۱۱a را بوجـود آورد. خوشـبختانه، ۸۰۲,۱۱a از همان MAC پیشینیان خود استفاده می کند، بنابراین بیشتر آنچه مدیران راجـع بـه ۸۰۲,۱۱ و تحلیـل کننده ها می دانند، بدرد می خورد. مدیران شبکه باید دنبال محصولی سازگار باشند که هر دو استاندارد ۸۰۲,۱۱a و ۸۰۲,۱۱b را بصورت یکجا و ترجیحاً به صورت همزمان پشتیبانی کند. چیپ ست هـای دوبانـدی ۸۰۲,۱۱a/b و کارت های ساخته شده با آنها به آنالایزرها اجازه می دهد که روی هر دو باند بدون تغییـرات سـخت افـزاری کـار کنند، و این بدین معنی است که مدیران شبکه نیاز به خرید و آموزش فقط یک چارچوپ پشتیبانی شده برای هر دو استاندارد دارند. این روال باید تا ۸۰۲,۱۱g ادامه یابد، تا جایی که سازندگان آنالایزرها کارت هـای ۸۰۲,۱۱a/b/g را مورد پذیرش قرار دهند.



بسیاری از ابزارها می توانند برای انجام امور رسیدگی به سایت و ردیابی نقاط دسترسی نامطلوب استفاده شوند، اما مدیران شبکه باید از نیاز به همگامی با آخرین تکنیک های استفاده شده در این بازی موش و گربه! آگاه باشند. نقاط دسترسی می توانند در هر باند فرکانسی تعریف شده در ۸۰۲,۱۱ بکارگرفته شوند، بنابراین مهم است که تمام ابزارهای مورد استفاده در بررسی های سایت بتوانند کل محدوده فرکانسی را پویش کنند. حتی اگر شما استفاده از ۸۰۲,۱۱b را انتخاب کرده اید، آنالایزر استفاده شده برای کار نظارت بر سایت، باید بتواند همزمان نقاط دسترسی ۸۰۲,۱۱a را نیز پویش کند تا در طول یک بررسی کامل نیازی به جایگزین های سخت افزاری و نرم افزاری نباشد. بعضی نقاط دسترسی نامطلوب سعی دارند کانالهایی را به صورت غیرقانونی روی کانال های ۸۰۲,۱۱b به کار بگیرند که برای ارسال استفاده نمی شوند. برای مثال قوانین FCC تنها اجازه استفاده از کانال های ۱ تا ۱۱ از ۸۰۲,۱۱b را می دهد. کانال های ۱۲ تا ١٤ جزء مشخصات آن تعریف شده اند اما فقط برای استفاده در اروپا و ژاپن کاربرد دارند. به هرحال، بعضی کاربران ممکن است از نقطه دسترسی کانال های اروپایی یا ژاپنی استفاده کنند، به این امید که رسیدگی یک سایت متمرکز روی کانال های مطابق با FCC از کانال های فرکانس بالاتر چشم پوشی کند. این قضیه مخصوصاً برای ردیابی ابزارهایی اهمیت دارد که بیرون باند فرکانسی مجاز بکارگرفته شده اند تا از اعمال اجرایی اتخاذ شده توسط نمایندگی های مجاز برحذر باشند. آنالایزرهای غیرفعال (Passive Analyzers) ابزار ارزشمندی هستند زیرا استفاده های غیرمجاز را تشخیص می دهند، اما چون توانی ارسال نمی کنند استفاده از آنها قانونی است.

مدیران شبکه همواره تحت فشار زمانی هستند، و به روش آسانی برای یافتن نقاط دسترسی نامطلوب و در عین حال چشم پوشی از نقاط دسترسی مجاز نیاز دارند. موتورهای جستجوی خبره به مدیران اجازه می دهند که لیستی از نقاط دسترسی مجاز را پیکربندی کنند. هر نقطه دسترسی غیرمجاز باعث تولید علامت هشدار دهنده ای می شود. در پاسخ به علامت هشدار دهنده، مدیران شبکه می توانند از ابزار دیگری برای پیدا کردن نقطه دسترسی براساس مقیاس های قدرت سیگنال استفاده کنند. اگرچه این ابزارها ممکن است خیلی دقیق نباشند، ولی برای محدود کردن محوطه جستجوی نقطه دسترسی نامطلوب به اندازه کافی مناسب هستند.

مسأله شماره ۳: استفاده غیرمجاز از سرویس

چندین شرکت مرتبط با شبکه های بی سیم نتایجی منتشر کرده اند که نشان می دهد اکثر نقاط دسترسی با تنها تغییرات مختصری نسبت به پیکربندی اولیه برای سرویس ارائه می گردند. تقریباً تمام نقاط دسترسی که با پیکربندی پیش فرض مشغول به ارائه سرویس هستند، WEP (Wired Equivalent Privacy) را فعال نکرده اند یا یک کلید پیش فرض دارند که توسط تمام تولیدکنند گان محصولات استفاده می شوند. بدون WEP دسترسی به شبکه به راحتی میسر است. دو مشکل به دلیل این دسترسی باز می تواند بروز کند: کاربران غیرمجاز لزوماً از مفاد ارائه سرویس تبعیت نمی کنند، و نیز ممکن است تنها توسط یک اسپم ساز اتصال شما به ISPتان لغو شود.

راه حل شماره۳ : طراحی و نظارت برای تأیید هویت محکم

راه مقابله مشخص با استفاده غیرمجاز، جلوگیری از دسترسی کاربران غیرمجاز به شبکه است. تأیید هویت محکم و محافظت شده توسط رمزنگاری یک پیش شرط برای صدور اجازه است، زیرا امتیازات دسترسی برپایه هویت کاربر قرار دارند. روش های VPN که برای حفاظت از انتقال در لینک رادیویی به کارگرفته می شوند، تأیید هویت محکمی را ارائه می کنند. تخمین مخاطرات انجام شده توسط سازمان ها نشان می دهد که دسترسی به ۸۰۲,۱X باید توسط روش های تأیید هویت برپایه رمزنگاری تضمین شود. از جمله این روش ها می توان به TLS (Layer Security Transport)، TTLS (Tunneled TLS) یا PEAP (Protected Extensible Authentication Protocol) اشاره کرد.

هنگامی که یک شبکه با موفقیت راه اندازی می شود، تضمین تبعیت از سیاست های تایید هویت و اعطای امتیاز مبتنی بر آن حیاتی است. همانند مسأله نقاط دسترسی نامطلوب، در این راه حل نیز نظارت های منظمی بر تجهیزات شبکه بی سیم باید انجام شود تا استفاده از مکانیسم های تأیید هویت و پیکربندی مناسب ابزارهای شبکه تضمین شود. هر ابزار نظارت جامع باید نقاط دسترسی را در هر دو باند فرکانسی b۸۰۲,۱۱ (باند ۲,٤ GHz ISM) و a۸۰۲,۱۱ (٥ GHz U-NII) تشخیص دهد و پارامترهای عملیاتی مرتبط با امنیت را نیز مشخص کند. اگر یک ایستگاه غیرمجاز متصل به شبکه کشف شود، یک رسیور دستی می تواند برای ردیابی موقعیت فیزیکی آن استفاده شود. آنالایزرها نیز می توانند برای تأیید پیکربندی بسیاری از پارامترهای نقاط دسترسی استفاده گردند و هنگامی که نقاط دسترسی آسیب پذیری های امنیتی را نمایان می کنند، علائم هشدار دهنده صوتی تولید کنند.

مسأله شماره ۴ : محدودیت های سرویس و کارایی

LANهای بی سیم ظرفیت های ارسال محدودی دارند. شبکه های ۸۰۲,۱۱b سرعت انتقالی برابر بـا Mbps ۱۱ و شبکه های برپایه تکنولوژی جدید ۸۰۲,۱۱a نرخ انتقال اطلاعاتی تا Mbps ٥٤ دارند. البته ماحصل مـؤثر واقعـی، به دلیل بالاسری لایه MAC، تقریباً تا نیمی از ظرفیت اسمی می رسد. نقاط دسترسی کنونی این ظرفیت محـدود را بین تمام کاربران مربوط به یک نقطه دسترسی قسمت می کنند. تصور اینکه چگونه برنامه های محلی احتمالاً چنین ظرفیت محدودی را اشغال می کنند یا چگونه یک نفوذگر ممکن است یک حمله انکار سرویس (DoS) روی ایـن منابع محدود طرح ریزی کند، سخت نیست.

ظرفیت رادیویی می تواند به چندین روش اشغال شود. ممکن است توسط ترافیکی کـه از سـمت شـبکه باسـیم بـا نرخی بزرگتر از توانایی کانال رادیویی می آید، مواجه شود. اگر یـک حملـه کننـده یـک ping flood را از یـک بخش اترنت سریع بفرستد، می تواند به راحتی ظرفیت یک نقطه دسترسی را اشغال کند. با اسـتفاده از آدرس هـای broadcast امکان اشغال چندین نقطه دسترسی متصل به هم وجود دارد. حمله کننده همچنین می تواند ترافیـک را به شبکه رادیویی بدون اتصال به یک نقطه دسترسی بی سیم تزریق کند. ۸۰۲,۱۱ طوری طراحی شده است که به چندین شبکه اجازه به اشتراک گذاری یک فضا و کانال رادیویی را می دهد. حمله کنندگانی که می خواهنـد شـبکه بی سیم را از کار بیاندازند، می توانند ترافیک خود را روی یک کانال رادیویی ارسال کنند و شـبکه مقـصد ترافیـک جدید را با استفاده از مکانیسم CSMA/CA تا آنجا که می تواند می پذیرد. مهاجمان بداندیش که فریم های ناسالم می فرستند نیز ظرفیت محدود را پر می کنند. همچنین ممکن است مهاجمان تکنیک های تولید پارازیت رادیویی را انتخاب کنند و اقدام به ارسال اطلاعات با نویز بالا به شبکه های بی سیم مقصد کنند.

بارهای بزرگ ترافیک الزاماً با نیات بدخواهانه تولید نمی شوند. انتقال فایل های بزرگ یا سیستم client/server ترکیبی ممکن است مقادیر بالایی از دیتا روی شبکه ارسال کنند. اگر تعداد کافی کاربر شروع به گرفتن انـدازه هـای بزرگی از دیتا از طریق یک نقطه دسترسی کنند، شبکه شبیه سازی دسترسی dial-up را آغاز می کند.

راه حل شماره۴ : دیدبانی شبکه

نشان یابی مسائل کارایی با دیدبانی و کشف آنها آغاز می شود. مدیران شبکه بـسیاری از کانـال هـا را بـرای کـسب اطلاعات در مورد کارایی در اختیار دارنـد: از ابزارهـای تکنیکـی خـاص ماننـد SNMP (Simple Network

(Management Protocol گرفته تا ابزارهای بالقوه قوی غیرفنی مانند گزارش های کارایی کـاربران. یکـی از مسائل عمده بسیاری از ابزارهای تکنیکی، فقدان جزئیات مورد نیاز برای درک بسیاری از شکایت های کـاربران در مورد کارایی است. آنالایزرهای شبکه های بی سیم می توانند با گزارش دهی روی کیفیت سیگنال و سلامت شـبکه در مکان کنونی خود، کمک باارزشی برای مدیر شبکه باشند. مقادیر بالای ارسال های سرعت پایین می تواند بیانگر تداخل خارجی یا دور بودن یک ایستگاه از نقطه دسترسی باشد. توانایی نشان دادن سرعت های لحظه ای روی هـر کانال، یک تصویر بصری قوی از ظرفیت باقی مانده روی کانال می دهد که به سادگی اشـغال کامـل یـک کانـال را نشان می دهد. ترافیک مفرط روی نقطه دسترسی می تواند با تقسیم ناحیه پوشش نقطه دسترسی به نواحی پوشـش کوچک تر یا با اعمال روش شکل دهی ترافیک در تلاقی شبکه بی سیم با شبکه اصلی تعیین شود.

در حالیکه هیچ راه حل فنی برای آسیب پذیری های ناشی از فقدان تأیید هویت فریم های کنترل و مدیریت وجـود ندارد، مدیران می توانند برای مواجهه با آنها گام هایی بردارنـد. آنالایزرهـا اغلـب نزدیـک محـل هـای دردسرسـاز استفاده می شوند تا به تشخیص عیب کمک کنند و به صورت ایده آل برای مشاهده بسیاری از حملات DoS کـار گذاشته می شوند. مهاجمان می توانند با تغییر دادن فریم های ۸۰۲,۱۱ با استفاده از یکـی از چنـدین روش معمـول واسط های برنامه نویسی ۸۰۲,۱۱ موجود، از شبکه سوءاستفاده کنند. حتی یک محقق امنیتی ابزاری نوشته است کـه پیام های قطع اتصال فرستاده شده توسط نقاط دسترسی به کلاینت ها را جعل می کند. بدون تأیید هویت پیام های قطع اتصال بر اساس رمزنگاری، کلاینت ها به این پیام های جعلی عمل می کنند و اتصال خود را از شبکه قطع می کنند. تا زمانی که تأیید هویت به صورت یک فریم رمزشده استاندارد درنیاید، تنها مقابله علیه حمـلات جعـل پیـام، مکان یابی حمله کننده و اعمال عکس العمل مناسب است.

سه روش امنیتی در شبکه های بی سیم عبارتند از :

- WEP(Wired Equivalent Privacy)

در این روش از شنود کاربرهایی که در شبکه مجوز ندارند جلوگیری به عمل می آید که مناسب برای شبکه هـای کوچک بوده زیرا نیاز به تنظیمات دستی(KEY) مربوطه در هر Client می باشد.

اساس رمز نگاری WEP بر مبنای الگوریتم RC٤ بوسیله RSA می باشد.

- **SSID** (**Service Set Identifier**)

شبکه های WLAN دارای چندین شبکه محلی می باشند که هر کدام آنها دارای یک شناسه (Identifier) یکتا می باشند این شناسه ها در چندین Access Point قرار داده می شوند . هر کاربر برای دسترسی به شبکه مورد نظر بایستی تنظیمات شناسه SSID مربوطه را انجام دهد .

- **MAC** (**Media Access Control**)

لیستی از MAC آدرس های مورد استفاده در یک شبکه به AP (Access Point) مربوطه وارد شده بنابراین تنها کامپیوترهای دارای این MAC آدرسها اجازه دسترسی دارند به عبارتی وقتی یک کامپیوتر درخواستی را ارسال می کند MAC آدرس آن با لیست MAC آدرس مربوطه در AP مقایسه شده و اجازه دسترسی یا عدم دسترسی آن مورد بررسی قرار می گیرد .این روش امنیتی مناسب برای شبکه های کوچک بوده زیرا در شبکه های بزرگ امکان ورود این آدرسها به AP بسیار مشکل می باشد.

امن سازی شبکه های بیسیم:

با وجود امکاناتی که در شبکه های مبتنی بر ۸۰۲,۱۱ ارائه شده است ولی این واقعیت وجود دارد که، چون برای انتقال اطلاعات در این شبکه ها هیچ حد و مرز فیزیکی وجود ندارد و این ترافیک توسط هوا منتقل می شود به این دلیل این نوع شبکه ذاتاً نا امن هستند.

از تمام عناصری که برای ایجاد امنیت در شبکه سیم کشی شده استفاده شده می توان در شبکه های بیسیم نیز برای برقراری امنیت استفاده نمود. نکته مهمی که در شبکه های بیسیم از لحاظ امنتی دارای اهمیت می باشد طراحی این گونه از شبکه های می باشد. در ادامه به چگونگی طراحی امن شبکه های بیسیم می پردازیم.

طراحی شبکه:

یکی از موارد مهم که در طراحی شبکه می بایست در نظر گرفته شود، چگونگی طراحی و نحوه ارتباط با شبکه سیم کشی شده است.

راههای زیادی جهت امن کردن شبکه و همین طور برای به خطر انداختن امنیت آن وجود دارد.

با طراحی و بکار گیری یک استراتژی محکم در شبکه های بیسیم میتوان از دسترسی هکرها به شبکه جلوگیری بعمل آورد همچنین با اعمال کنترل های بیشتر روی بخش بیسیم شبکه، شبکه سیم کشی شده را نیز محافظت نمود

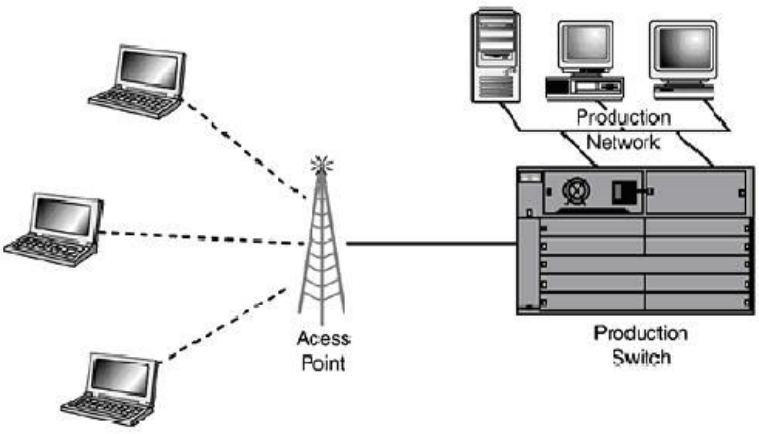
تا هکرها از این طریق نیز نتوانند وارد شبکه شوند. استفاده از فایروال و روتر در شبکه بیسیم همانند شبکه های سیم کشی شده نیز توصیه می شود.

جداسازی توسط مکانیزم های جداسازی:

بهدلیل اینکه معمولاً AP ها رابط بین شبکه بیسیم و سیم کشی شده هستند، ایستگاه های کاری موجود در دو طرف این AP ها معمولاً در یک Broadcast Domain می باشند. با این توضیحات، هکر شبکه بیسیم میتواند با استفاده از روشهای موجود روی شبکه های سیم کشی شده مانندARP cache Poisoning نسبت به اجرای Exploit روی ترافیک Broadcast اقدام نماید. همچنین هکر می تواند ایستگاه های بیسیم دیگری را که به AP متصل هستند را مورد حمله قرار دهد. این اتفاق در مورد ایستگاه های کاری موجود روی شبکه سیم کشی شده که به شبکه بیسیم متصل هستند روی خواهد داد.

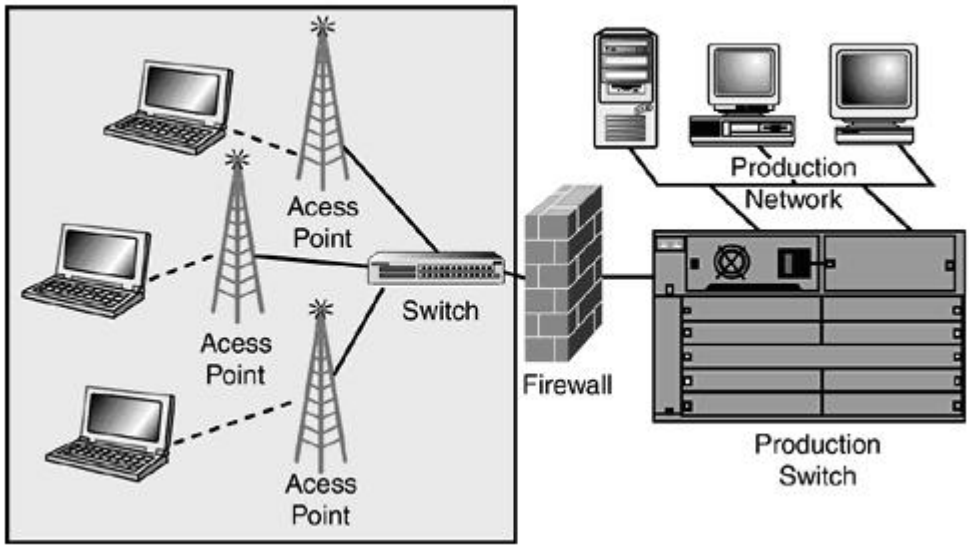
به دلیل آسیب پذیری های زیادی که در شبکه های بیسیم و با توجه به نحوه پیاده سازی این شبکه ها، این فکر در ذهن ایجاد می شود که شبکه های سیم کشی ایزوله شده از این شبکه ها امن تر می باشند.

همانطوری که در شکل زیر مشاهده میشود، طراحی ساده ولی با یک نکته اصلی و آن اینکه، در این طرح، دسترسی مستقیم لایه ۲ و اتصال به منابع شبکه برای تمامی ایستگاه های کاری بیسیم میسر می شود و این امر مشکلات امنیتی را در پی خواهد داشت. حداقل پیشنهادی که برای امنیت در این طرح مورد نظر می باشد، جدا سازی و ایزوله کردن شبکه بیسیم از شبکه داخلی در VLAN جداگانه و با قرار دادن مکانیزم های لایه ۳ در شبکه می باشد.



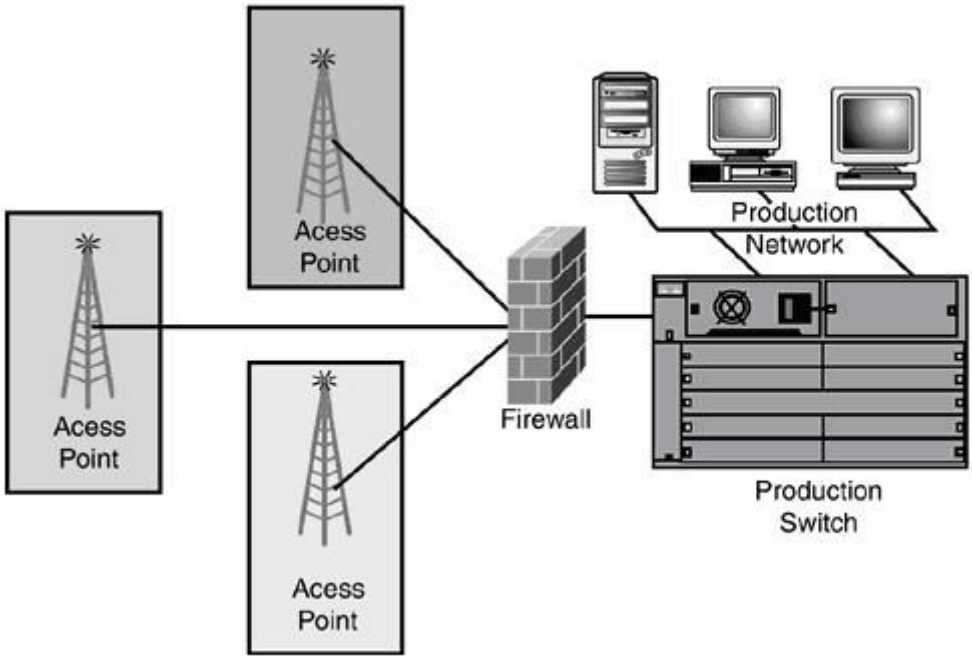
طراحی بهتر شبکه با درک مفهوم Wireless-DMZ که در شکل زیر نشان داده شده است انجام خواهد شد. با قرار دادن APها در ناحیه امنیت خاص، پیاده سازی کنترل های لایه۳ و کنترل های دسترسی مانند پیاده سازی فایروال می توان به امنیت بالاتری دست یافت.

به طور مثال اگر تمام AP ها به یک سوئیچ (یا دو سوئیچ برای افزونگی(Redundancy)) متصل و سپس سوئیچ به فایروال متصل شود، ما یک نقطه کنترلی یا +۳ Layer بین شبکه داخلی و شبکه AP خواهیم داشت.



با توجه به شبکه فوق، اگر هکری ایستگاه های بیسیم و یا حتی AP ها را تحت کنترل خود در آورد، محدود به شبکه خود (شبکه خارج از فایروال) و به سرویسهایی که در فایروال باز گذاشته شده می باشد. بعلاوه هرگونه ترافیک ورودی و خروجی در فایروال ثبت شده و بدین ترتیب ما رد ممیزی حتی و با بررسی این گزارشات شانس بیشتری برای جلوگیری از حملات خواهیم داشت.

و اگر AP ها دارای رده امنیت مختلفی باشند می توان هرکدام را در ناحیه امنیتی خود قرار داده و به فایروال مربوطه با چند interface مطابق شکل زیر متصل نمود. با این طرح منابع هرکدام از شبکه های بیسیم در مقابل شبکه های دیگر محافظت می شود.



محافظت در برابر ضعف های ساده:

ساختار شبکه های بیسیم، اصولا نسبت به حملات ضعف دارد.بدین صورت که دسترسی به اطلاعات شبکه بیسیم را از طریق AP ها و حتی شبکه های مبتنی بر سیم متصل به آن را، به حمله کننده می دهد. از حملات متداول، دسترسی لایه ۲ حمله کننده به شبکه بدون نفوذ فیزیکی به شبکه می باشد. برای جلوگیری از این ضعف امواج ۸۰۲,۱۱، می بایست قرار گیری AP ها و جهت آنتن های آنها را طوری طراحی کرد تا دامنه امواج آن محدود به شبکه داخلی داشته باشد. همچنین استفاده از پنجره ها و دیوارهای عایق بندی شده به ضعیف کردن امواج خروجی کمک می کند یا میتوان محلی را که امواج درآن نقطه ارسال می شود را جزو محدوده کنترلی شبکه و به صورت فیزیکی کنترل نمود. واضح است که هرچه دسترسی از شبکه عمومی به شبکه محلی کمتر و محدود تر باشد، شبکه از امنیت بالاتری برخوردار می باشد.

کنترل در برابر حملات DoS:

این حمله باعث کند شدن، از کار افتادن سرویس بیسیم(بسته به نوع طراحی شبکه) و یا تاثیر روی شبکه اصلی خواهد شد. بیشتر شرکت ها، دستگاه های ردیاب این نوع از حملات را ندارند اگر چه امروزه نرم افزارهایی برای این کار در دسترس می باشد مانند Airmagnet.

جدا سازی DoS از شبکه داخلی با استفاده از فایروال یا دستگاه های دیگری که دارای این قابلیت هستند نیز می تواند در مقابله با حمله DoS موثر باشد.

کنترل های QoS می تواند در لبه wireless DMZ پیاده سازی شود حس گرهای IDS می بایست در نقطه ارتباط بین شبکه بیسیم و شبکه مبتنی بر سیم قرارگیرد و در نهایت روشی کامل برای جلوگیری ازDoS وجود ندارد و طراحی درست با در نظر گرفتن موارد امنیتی میتواند خطر این نوع حمله را کاهش دهد.

رمزنگاری شبکه بیسیم:

اگرچه در شبکه های سیم کشی شده از رمزنگاری در لایه ۱و۲ استفاده نمی شود ولی طراحان ۸۰۲,۱۱ نوعی مکانیزم رمزنگاری را جهت امکان تشخیص هویت و رمزنگاری را بین دو ایستگاه کاری روی لایه ۱و۲ فراهم ساخته اند.

رمزنگاری بیسیم به معنی محافظت و محدود کردن دسترسی به منابع و ساختار شبکه بیسیم می باشد این کار برای محافظت در برابر خاصیت بیسیم است که از دیوار و سایر موانع فیزیکی عبور می کند. حمله کننده براحتی می تواند به شبکه بیسیم که سیستم های کد گذاری و محدودیت های دسترسی پیاده سازی نشده راه پیدا کند. در شناسایی های به عمل آمده در سال ۲۰۰۱ در Boston از هر ۱۰۰ شبکه بیسیم ٤٤ شبکه با سیستم های رمزنگاری پیاده سازی شده اند.

به خاطر داشته باشید که پیاده سازی هرنوع رمزنگاری از نداشتن آن بهتر است.

واضح است که اگرحمله کننده ای با دو شبکه که یکی دارای رمزنگاری ضعیف و دیگری بدون رمزنگاری باشد مواجه باشد، به شبکه ای که بدون رمزنگاری است حمله خواهد کرد.

: Wired equivalent privacy (WEP)

از بخشهای مهم امن کردن شبکه بیسیم، استفاده از الگوریتم مناسب رمزنگاری برای محافظت از اطلاعاتی است که در هوا منتشر میشود.

WEP برای امن کردن ارتباط بین کارت شبکه های بیسیم و AP ها، بوجود آمد. ویرایش اصلی آن قابلیت پشتیبانی از کلیدهای ٤٠ بیتی یا ٦٤ بیتی را داشت که در ویرایش های بعدی(WEP٢) پشتیبانی ١٢٨ بیتی نیز به آن اضافه گردید. WEP ازالگوریتم RC٤ برای رمزنگاری استفاده میکند که خود دارای ضعف هایی نیز می باشد و حمله کننده میتواند با بکارگیری روش ها و نرم افزارهای خاص، نظیرWEP crack و Air Snort برای رمزگشایی آنها استفاده نماید.اگر چه WEP دارای ضعف هایی میباشد، همچنان استفاده میشود. اگرWEP تنها انتخاب شما برای رمزنگاری میباشد بهتر است که از آن استفاده نمایید و شبکه بدون رمزنگاری را پیاده سازی نکنید. بعضی از سازندگان تجهیزات بیسیم، با اضافه کردن LEAP، که یک پروتکل تشخیص هویت میباشد، به WEP و استفاده در تجهیزات خود، ضعف WEP را پوشش داده اند.

محکم سازی AP ها:

مانند شبکه های سیم کشی شده که روتر نقش ورودی شبکه از اینترنت را بازی میکند، در شبکه های بیسیم نیز APها نقش ارتباط بین دو شبکه سیم کشی شده و بیسیم را برقرارمی کند.

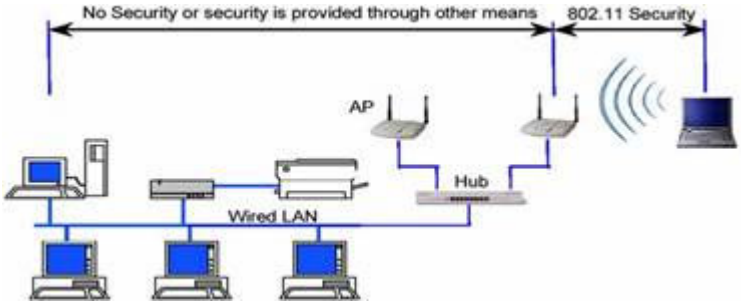
چندین راه برای محکم سازی AP ها وجود دارد مانند:

down SSID Broadcast Shutting
MAC addresses Locking down
unused services Disabling
Password Strong

قابلیت‌ها و ابعاد امنیتی استاندارد۱۱ . ۸۰۲

استاندارد ۸۰۲,۱۱ سرویس‌های مجزا و مشخصی را برای تأمین یک محیط امن بی‌سیم در اختیار قرار می‌دهد. این سرویس‌ها اغلب توسط پروتکل WEP (Wired Equivalent Privacy) تأمین می‌گردند و وظیفه‌ی آن‌ها امن‌سازی ارتباط میان مخدوم‌ها و نقاط دسترسی بی‌سیم است. درک لایه‌یی که این پروتکل به امن‌سازی آن

می‌پردازد اهمیت ویژه‌یی دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و بـه لایـه‌هـای دیگـر، غیـر از لایه‌ی ارتباطی بی‌سیم که مبتنی بر استاندارد ۸۰۲,۱۱ است، کاری ندارد. این بدان معنی است کـه اسـتفاده از WEP در یک شبکه‌ی بی‌سیم به‌معنی استفاده از قابلیت درونی استاندارد شبکه‌های محلی بی‌سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.



شکل قبل محدوده‌ی عمل کرد استانداردهای امنیتی ۸۰۲,۱۱ (خصوصاً WEP) را نشان می‌دهد.

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه‌هـای بـی‌سـیم بـر اسـاس اسـتاندارد ۸۰۲,۱۱ فراهم می‌کند WEP است. این پروتکل با وجود قابلیت‌هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه‌های بی‌سیم را به نحوی، ولو سخت و پیچیده، فراهم می‌کند. نکته‌یی که باید به‌خاطر داشـت ایـن‌سـت کـه اغلب حملات موفق صورت گرفته در مورد شبکه‌های محلی بی‌سیم، ریشه در پیکربندی ناصحیح WEP در شـبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می‌گذارد، هرچنـد که فی‌نفسه دچار نواقص و ایرادهایی نیز هست.

بسیاری از حملاتی که بر روی شبکه‌های بی‌سیم انجام می‌گیرد از سویی است که نقاط دسترسی با شـبکه‌ی سـیمی دارای اشتراک هستند. به عبارت دیگر نفوذگران بعضاً با استفاده از راه‌های ارتباطی دیگری که بر روی مخدوم‌هـا و سخت‌افزارهای بی‌سیم، خصوصاً مخدوم‌های بی‌سیم، وجود دارد، به شبکه‌ی بی‌سیم نفوذ می‌کننـد کـه ایـن مقولـه نشان دهنده‌ی اشتراکی هرچند جزءیی میان امنیت در شبکه‌های سیمی و بی‌سـیم‌یـی‌سـت کـه از نظـر سـاختاری و فیزیکی با یکدیگر اشتراک دارند.

سه قابلیت و سرویس پایه توسط IEEE برای شبکه‌های محلی بی‌سیم تعریف می‌گردد :

Authentication

هدف اصلی WEP ایجاد امکانی برای احراز هویت مخدوم بی‌سیم است. این عمل که در واقع کنترل دسترسی به شبکه‌ی بی‌سیم است. این مکانیزم سعی دارد که امکان اتصال مخدوم‌هایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد.

Confidentiality

محرمانه‌گی هدف دیگر WEP است. این بُعد از سرویس‌ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه‌های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه‌ی محلی بی‌سیم است.

Integrity

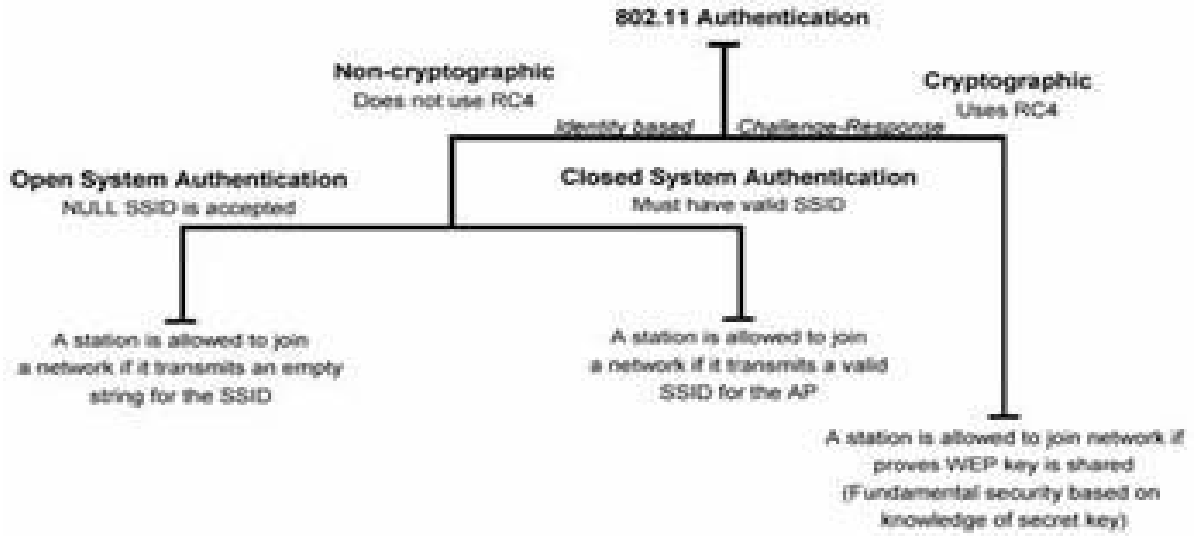
هدف سوم از سرویس‌ها و قابلیت‌های WEP طراحی سیاستی است که تضمین کند پیام‌ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان مخدوم‌های بی‌سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی‌گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه‌های ارتباطاتی دیگر نیز کم‌وبیش وجود دارد.

Authentication

استاندارد ۸۰۲,۱۱ دو روش برای احراز هویت کاربرانی که درخواست اتصال به شبکه‌ی بی‌سیم را به نقاط دسترسی ارسال می‌کنند، دارد که یک روش بر مبنای رمزنگاری‌ست و دیگری از رمزنگاری استفاده نمی‌کند.

شکل زیر شَمایی از فرایند Authentication را در این شبکه‌ها نشان می‌دهد

!Error



۴– تکنولوژی WIFI

۴-۱تکنولوژی رادیویی **WIFI**

۴-۲شبکه **. Walkie_Talkie**

۴-۳به‌کارگیری وای‌فای در صنعت تلفن همراه

۴-۴آنچه شما نیاز دارید برای ساختن یک شبکه بیسیم

۴-۵ترکیب سیستم **Wi-Fi** با رایانه

۴-۶به شبکه های **WiFi** باز وصل نشوید.

۴-۷آگاهی و درک ریسک ها و خطرات **WIFI**

۴-۸استفاده از تکنولوژی **MIMO** جهت افزایش سرعت **WiFi** زیر دریا

مقدمه

سیستم رادیویی که در وای فای استفاده می شود با انچه در دستگاه مخابره رادیویی استفاده می شود چندان متفاوت نیست .آن ها قادر هستند مخابره و دریافت کنند .می توانند صفر ها ویک ها را بـه امـواج رادیـویی تبـدیل کننـد و سپس آن ها را دوباره به صفر و یک تبدیل کنند .

تکنولوژی رادیویی WIFI

سه تفاوت عمده بین سیستم رادیویی وای فای و یک دستگاه مخابره کوچک وجود دارد :

سیستم وای فای که با استاندارد ۸۰۲,۱۱B و ۸۰۲,۱۱g کار میکند در فرکانس ۲/٤ گیگاهرتز عمل می کندو آنهـایی که با ستاندارد ۸۰۲,۱۱aکار می کنند در فرکانس ۵ گیگاهرتز ارسال می کنند . در حـالی کـه یـک دسـتگاه مخـابره کوچک د رفرکانس ٤۹ مگاهرتز عمل می کند .فرکانس بابلاتر موجب افزایش سرعت انتقال اطلاعات می شود .

برای استاندارد ۸۰۲,۱۱a و ۸۰۲,۱۱g از تکنیک OFDM استفاده می شودو برای استاندارد ۸۰۲,۱۱b از تکنیـک CCK استفاده می شود.

سیستم رادیویی استفاده شده در وای فای توانایی تغییر فرکانس را دارد .۸۰۲,۱۱b می توانند در هر سه باند مخـابره کنند یا می توانند پهنای رادیویی در دسترس را به دوازده کانال تقسیم کنند و جهش فرکانسی به سـرعت بـین آنهـا انجام شود. مزیت جهش فرکانسی این است که باعث تداخل کمتر می شود و اجازه می دهد که چندین کارت وای فای به طور همزمان بدون تداخل با یکدیگر مداخله کنند .بنابراین سیستم رادیویی وای فای می تواند میـزان بـسیار زیادی از اطلاعات را در هر ثانیه مخابره کند.

کارت های ٦۰۲,۱۱ bمیتوانند مسیقیماً بر روی هر یک از این سه باند ارسـال شـوند ، یـا مـی تواننـد پهنـای باننـد رادیویی در دسترس را به چندین کانـال و hop frequency بـین آنهـا تبـدیل کننـد . مزیـت frequency hoppingدر این است که در مقابل اختلال و پارازیت بسیار ایمن تر است و بـه چنـدین عـدد از کـارت هـای WiFiاجازه می دهد بطور همزمان و بدون ایجاد اختلال در کار هم با یکدیگر مکالمه کنند .

به دلایلی که ذکر شد، سیستم های رادیویی Wi-Fi ظرفیت و سرعت انتقال داده با لاتری را نسیت به رادیو هـای واکی – تاکی دارند، این سرعت ها برای استاندارد ۸۰۲,۱۱b تا ۱۱ مگابایت بر ثانیه و بـرای ۸۰۲,۱۱a و ۸۰۲,۱۱g در حدود ۳۰ مگابایت بر ثانیه است.

شبکه : Walkie_Talkie

اگر می خواهید با شبکه سازی بیسیم در ساده ترین سطح آن آشنا شـوید ، یـک جفـت Walkie_Talkie ارزان قیمت ۵ دلاری را در نظر بگیرید . اینها رادیوهای کوچکی هستند که قادر به ارسال و دریافت امـواج رادیـویی مـی باشند . وقتی در یک Walkie_Talkie صحبت می کنید ، صدای شما توسط یک میکروفون دریافت می شـود . سپس به شکل یک فرکانس رادیویی کد گذاری می شود و توسط آنتن آن ارسال می گردد Walkie_Talkie . دیگر می تواند امواج ارسال شده را توسط آنتن خود دریافت کند ، صدای شما را که به شکل امـواج رادیـویی کـد گذاری شده decode کند و آن را از یک بلند گو پخش نماید . یک Walkie_Talkie نمونـه مثـل ایـن ، بـا قدرت سیگنالی در حدود ۰,۲۵ وات امواج را ارسال می کند و برد آنها می تواند و برد آنها می تواند به حدود ۵۰۰ تا ۱۰۰۰ فوت برسد .

بیایید تصور کنیم که شما قصد دارید دو کامپیوتر را با استفاده از تکنولوژی Walkie_Talkie در یک شبکه به هم وصل کنید :

شما هر دو کامپیوتر با یک Walkie_Talkie تجهیز می کنید . شما برای هر دو کامپیوتر روشی را برای مشخص نمودن اینکه آیا قصد ارسال یا دریافت امواج را دارد معین می نمایید .

شما روشی را بمنظور تبدیل کد های باینری (دودویی) ۰ و ۱ ها به دو beep متفاوت که Walkie_Talkie بتواند آنها را ارسال و دریافت کند و بین beep ها و ۰ و ۱ ها عمل تبدیل به انجام برساند مشخص می کنید . این سناریو عملاً کار می کند . تنها مشکلی که در این زمینه وجود دارد این است که نرخ تبادل داده بسیار آهسته و کند است . یک Walkie_Talkie ۵ دلاری برای کار با صدای انسان طراحی شده است ، بنابراین شما نمی توانید حجم زیادی از داده ها را به این روش ارسال کنید . شاید ۱۰۰۰ بیت در ثانیه .

به‌کارگیری وای‌فای در صنعت تلفن همراه

اشاره :

سازندگان گوشی‌های تلفن همراه همواره مشتاق هستند تا شما و دوستانتان را هر ساله به تعویض گوشی قدیمیتان با نمونه‌های جدید و مجهز به انواع امکانات پیشرفته ترغیب کنند. تا یک سال پیش از این، امکانات موجود روی یک گوشی همراه پیشرفته شامل دوربین عکاسی و پخش موسیقی بود. نسل پس از آن شامل دستگاهی می‌شد که با ضخامت بسیار کم به راحتی در جیب جای می‌گرفت و بالاخره در چند ماه گذشته پخش ویدیو آخرین گزینه‌ای

بود که بر صفحه نه چندان بزرگ گوشی‌های همراه ظاهر شد. با این وجود و به‌رغم معرفی انواع مدل‌های مختلف گوشی‌های همراه، مدل‌های باریک و ضخیم، گوشی‌های شکلاتی و تاشو، این وسیلهِ همیشه همراه، به طور بسیار ناراحت‌کننده‌ای ناکارآمد و ناقص به نظر می‌آید؛ به ویژه با اینترفیس‌های گیج‌کننده، عدم آنتن‌دهی مناسب و پیام‌های ناخواسته. آیا وقت آن نرسیده است که نوکیا با همکاری شرکت Cingular Wireless به این وضعیت پایان داده و باعث شوند تا این شبکه پر از وصله و رفو بهتر کار کند؟

در این رابطه هیچ‌کس قولی نمی‌دهد، اما سازندگان گوشی می‌گویند نسل بعدی فناوری تلفن‌های همراه که امسال معرفی خواهد شد، علاوه بر راحتی در استفاده، مشکلات کمتری در مسائل ارتباطی داشته و به خاطر دارا بودن امکان تبادل اطلاعات چندرسانه‌ای، ارزش امتحان کردن را دارد. همچنین صنعت موبایل امیدوار است به فناوری ساخت گوشی‌هایی دست یابد که بنا به گفته Rob N. Shaddock، مهندس ارشد بخش ابزارهای موبایل شرکت موتورولا، <کنترلی برای زندگی شما> محسوب گردند. این تصور جذابی است که بخواهیم یک گوشی هر کاری، از ضبط برنامه‌های تلویزیون گرفته تا بروزرسانی تقویم پی‌سی را انجام دهد؛ آن هم درحالی‌که شما سرگرم کارهای خود هستید.

این تصورات، جالب به نظر می‌رسند، اما بگذارید زیاده‌روی نکنیم. اگر تنها یک کار وجود داشته باشد که سازندگان این دستگاه‌ها مایل هستند صحیح انجام گیرد، این یک کار، بهتر انجام دادن همان وظیفه اصلی گوشی‌ها یعنی برقراری تماس خواهد بود. صنعت موبایل پاسخی برای این تمایل یافته است؛ پاسخی به نام وای‌فای. همان فناوری‌ای که شما را قادر می‌سازد توسط آن به صورت بی‌سیم پی‌سی‌های خود را به هم متصل کنید.

پهنای باند پشتیبان

در حال حاضر کیفیت ارتباط موبایل بستگی به موقعیت قرارگیری شما نسبت به آنتن BTS دارد و در مکان‌های مسقف نیز در خیلی از موارد نخواهید توانست از گوشی خود استفاده کنید. هیچ‌کس بهتر از شش میلیون کاربر در ایالات متحده که برای داشتن تحرک کامل دست از خطوط تلفن ثابت خود کشیدند، این مشکل را لمس نمی‌کند. پل آوبری ۳٤ ساله مدرس موسیقی و ساکن کانزاس‌سیتی می‌گوید: <در بیمارستان‌ها، در داخل آسانسورها و در

مدرسه تا زمانی‌که کنار یک پنجره قرار نگیرم، نمی‌توانم تماس خوبی داشته باشم. برای حل این مشکل نوکیا و موتورولا تصمیم گرفتند تا نقاط تماس (Hotspots) دوگانه شبکه وای‌فای را معرفی کنند و آن‌ها را در خانه‌ها، دفاتر، نقاط اتصال جاوا و هرجای دیگری که لازم باشد، نصب نمایند. اطلاعات گوشی‌های موبایل در مجاورت این نقاط تماس بدون بروز اختلال و مشکل از یک سیستم به سیستم دیگر منتقل خواهند شد. البته میزان موفقیت این فناوری در آینده مشخص خواهد گردید. <ترکیب شبکه‌های سلولی و وای‌فای یک ترکیب قدرتمند و کارا می‌باشد.> این گفته فرانک هانزلیک، مدیر گروه تجاری Wi-Fi Alliance، است.

از لحاظ تئوری، وای‌فای کاری بیش از پایدار ساختن تماس‌های تلفنی انجام خواهد داد. گوشی‌های دو حالته از دو طریق به اینترنت متصل می‌شوند و اتصال وای‌فای نیز سرعت پهن‌باند را ایجاد می‌نماید. شرکت T-Mobile دو مدل گوشی معرفی نموده که با آنتن‌های این شرکت کار می‌کنند. البته همانند تمام تجهیزات موبایل، مدل‌های نخستین ممکن است ایراداتی داشته باشند. ظرفیت و مدت دوام باتری عنصر مهمی تلقی می‌شود. برای مثال، وای‌فای جهت انتقال اطلاعات از یک کامپیوتر به کامپیوتر دیگر به وجود آمد. اما پرگویی و حرف زدن در تمام طول روز با تلفن، تمام نیروی باتری را مصرف می‌کند. سازندگان می‌گویند مدل‌های اولیه قادر خواهند بود چهار – پنج ساعت گفت‌وگو با استفاده از وای‌فای را پشتیبانی نمایند. آنان امیدوارند تا در انتها بتوانند به مرز هشت ساعت دست یابند. هانزلیک همچنین می‌گوید: <در ابتدا مشکلاتی وجود داشت، اما ما پیشرفت‌های خوبی در این زمینه داشته‌ایم. این موارد درباره سرویس‌های فعلی ویدیویی یعنی Live TV نیز صادق هستند.

مردم آن‌گونه که شرکت‌های بزرگ فعال در این حوزه یعنی Verizon Wireless،Mobile ESPN و Amp'd Mobile آرزویش را دارند، برای دریافت اشتراک مقابل این شرکت‌ها صف نمی‌کشند. با استفاده از خدمات Sprint Nextel Corp یا Cingular Wireless. بیشترین چیزی که عاید کاربر می‌شود، خبرهای کوتاه سی‌ان‌ان یا خلاصه اعلام نتایج لیگ بیسبال خواهد بود. با این‌حال، چنانچه عده‌ای درهمان زمان و در نزدیکی شما بخواهند همین کلیپ‌ها را مشاهده کنند، آن وقت چه اتفاقی می‌افتد؟ تصویر دریافتی یا محو می‌شود یا اصلاً دریافت نمی‌شود. پل کاتالانو شریک و متخصص شبکه‌های بی‌سیم از شرکت مشاور RelevantC Business

Group، می‌گوید: <در حال حاضر شما نمی‌توانید برنامه‌های یک شرکت کابلی را برای استفاده صدها کاربر روی شبکه سلولی پخش کنید.>

برای حل این مشکل، صنعت موبایل در حال سرمایه‌گذاری روی سیستم‌های جدید می‌باشد؛ مانند آنچه Qualcomm در دست ساخت دارد و همچنین شبکه رقیب دیگری که توسط نوکیا، اینتل، موتورولا و دیگران پشتیبانی می‌شود. این شرکت‌ها قول داده‌اند تا سیگنال‌های زنده تلویزیونی را همانند شبکه‌های کابلی و ماهواره‌ای در سطح وسیعی از کشور پخش نمایند. این سیستم‌ها در آن واحد توانایی پخش بیست تا سی کانال را دارند و طراحی آنان به شکلی است که قدرت کافی برای تماشای صحنه‌های پرتحرک مانند فوتبال و بسکتبال را فراهم میآورند. این ویژگی‌ای است که فناوری‌های فعلی قادر به انجام آن نیستند.Verizon Wireless انتظار دارد تا انتهای سال سرویس Qualcomm را در نیمی از بازار تحت کنترل خود گسترش دهد. اما عده کمی معتقدند که این سرویس همان‌گونه که پیش از این و در تبلیغات نشان داده شد کار کند و در انتها تبدیل به یک موفقیت چشمگیر گردد. علاوه برآن، وادار ساختن میلیون‌ها کاربر به این‌که گوشی تلفن خود را <نگاه> کنند، مستلزم این است که این گوشی‌ها کمتر شبیه <گوشی> باشند. مسلماً کار آسانی نخواهد بود تا وسیله‌ای در اندازه یک شکلات ساخته شود و کار کردن با آن به سادگی روشن‌کردن مایکروویو باشد.

اما سازندگان و طراحان به سختی در حال کار روی امکان حذف کلیدها و افزودن فرامین صوتی بیشتر می‌باشند. به جای فشردن چندین دکمه و سرگردانی در بین منوها به منظور جست‌وجو در مورد مسئله‌ای مثل جام جهانی، در گوشی‌های آینده با فشار دادن تنها یک کلید و بر زبان آوردن فرمان صوتیِ <جست‌وجوی جام جهانی>، پس از چند لحظه چندین لینک درباره این مطلب روی صفحه نمایش داده می‌شوند. زمان پاسخ‌دهی نیز کوتاه‌تر شده و به گفتهJohn C. Burris جانشین مدیریت محصولات Sprint Nextel، <حتی به اندازه یک کلیک هم منتظر نخواهید ماند. درخواست شما همانجا حاضر و آماده است. این‌هم قسمتی که منتظرش بودید؛ یعنی استفاده از گوشی موبایل به عنوان کنترل از راه دور جهانی. در آینده‌ای نه چندان دور محتویات شامل عکس‌های دیجیتالی، موسیقی، نمایش‌های تلویزیونی یا حتی فهرست‌های تماس پیش پا افتاده، به جای ذخیره روی یک پی‌سی ترجیحاً

روی اینترنت ذخیره خواهند شد. در این‌حال یک گوشی موبایل شما را قادر خواهد ساخت تا از هر جا به این اطلاعات دسترسی داشته باشید.

شما می‌توانید به وسیله آن عکس‌ها را روی پی‌سی خود یا یک تلویزیون بفرستید. همچنین می‌توانید از گوشی خود بخواهید تا در زمانی‌که در راه هستید، کلیپ ویدیویی را برای شما ذخیره کند. به همین شکل می‌توانید از گوشی برای گوش دادن به موسیقی دیجیتالی مورد علاقه خود در منزل استفاده نموده و در حالی‌که به سمت پارکینگ می‌روید، آهنگ‌ها را به ماشین خود انتقال دهید. در آخر شما قادر خواهید بود گوشی خود را آن‌گونه که تاکنون ممکن نبوده است سسفارشی‌سازی کنید. ما در این‌جا از یک تغییر کوچک در محدوده مد صحبت نمی‌کنیم. با آغاز سال جدید، شرکت‌هایی همچون Sprint و Verizon Wireless یک قدم حساس دیگر برخواهند داشت و کاربران تلفن‌های همراه را قادر می‌سازند تا صفحه گوشی خود را به هر اطلاعاتی که مایل هستند، مزین نمایند. کافی است گوشی را روشن کنید تا نتایج تیم ورزشی مورد علاقه خود یا آخرین قیمت‌های بورس را مشاهده نمایید. Burris می‌گوید: <اطلاعات در طول شب یا در مدت جابه‌جایی کاربر، به گوشی او ارسال می‌شود.> چه کسی می‌داند؟ شاید Sprint و دیگران بتوانند این‌کار را انجام دهند و اقتدار شبکه‌های ویدیویی زمینی بالاخره شکسته شود.

آنچه شما نیاز دارید برای ساختن یک شبکه بیسیم

برای ساختن یک شبکه بیسیم نیاز به چند عضو پایه دارید .معمول ترین شبکه های بی سیم شامل یک مسیر یاب یا دستگاه نقطه دستیابی(Wireless Access Point یا WAP)و کارت شبکه بی سیم (به تعداد کامپوتر های متصل به شبکه)هستند.به عنوان مثال فرض کنیم در حال پیکربندی یک شبکه بی سیم در خانه ای هستید که دو کامپیوتر رومیزی یک ارتباط اینترنت باند عریض و یک لپ تاپ دارد.گام اول بای ساخت شبکه آن است مسیر یاب بیسیم را به مودم باند عریض وصل کنید.وقتی مسیر یاب به درستی پیکربندی شود به دروتزهای به سوی اینترنت تبدیل می شود.به هر کامپیوتر وصل شده در پشت مسیر یاب یک نشانی IP ثبت شده داخلی اختصاص می یابد که معمولا در محدوده ۱۹۲,۱۶۸.x.x است.

مسیر یاب ترافیک ورودی از نشانی IP ثبت شده – که به وسیلهISP اختصاص می یابد را بر دوش می گیرد و آن داده ها را به نـشانی I P مقتـضی هـدایت مـی کنـد.ایـن خـصوصیت کـه بـه NATیـا (network Address Translation)مشهور است یک لایه پایه حفاظتی بین کامپیوتر های شما و اینترنت به وجود می آورد.

پس از پیکربندی مسیریاب گام بعدی نصب کارتهای شبکه بی سیم در هر کامپیوتر شبکه است.کارتهای شبکه هـای بیسیم در انواع متنوعی عرضه شده اند.بعضی از آن کارتهای متداول PCI که شـبیه بـه سـایر کارتهـای PCI ماننـد کارتهای صذا نصب می شوند.

بعضی دیگر بای لپ تاپ هاساخته شده اند و از استاندارد PCMCIA تبعیت می کنند. اگر پی سی یا نـوت بـوک شما حاوی شکاف(slot)اضافی نباشد می توانید از آداپتورهای بی سیم USB بهره بگیریـد.نـصب آداپتـور شـبکه معمولا آسان است .آن را در یک شکاف خالی فرو کنیـدیا اگـر از نـوع USBاسـت رابطـه آن را بـه یـک درگـاه USBوصل کنید.سپس وقتی کامپیوتر خود را رئشن می کنید سیستم عامل باید این وسیله جدید را شناسایی کند و دستگاه رانهای(driver)جدید را نصب کند.دستگاه رانها معمولا بر روی یـک سـی دی یـا دیـسکت قـرار دارنـدو ویندوز می تواند آنها را شناساییو برای آداپتور نصب کند.وقتی دستکاه رانها نصب شدند کامپیوتر را باز راه انـدازی کنید و برنامه خدماتی ارتباط بی سیم را که به همراه آداپتور عرضه شده است رابرای پیداکردن امواج هوایی مربـوط به مسیر یاب به اجرا در آورید.(ویندوز اکس پی خود امکاناتی برای اداره ارتباطات شبکه بی سـیم دارد.)اگـر همـه چیز درست کار کند و شما در برد موثر شبکه باشید مسیر یاب باید در یک فهرست به عنوان یـک ارتبـاط موجـود ظاهر شود روی دکمهconnection کلیک کنید و کار برپایی شبکه تمام است.

ترکیب سیستم Wi-Fi با رایانه

امروزه اغلب رایانه های لپ تاپ مجهز به سیستم Wi-Fi داخلی هستند و در غیر این صورت نیازمنـد نـصب یـک کارت Wi-Fi بر روی لپ تاپ و یا رایانه رومیزی خود خواهیم بود. شما می توانید یک کارت Wi-Fi در سیـستم ۸۰۲,۱۱a یا ۸۰۲,۱۱b و یا ۸۰۲,۱۱g تهیه کنید که البته نـوع ۸۰۲,۱۱g نـسبت بـه تجهـزات ۸۰۲,۱۱b از سـرعت بالاتری برخوردار است. برای لپ تاپ ها این تجهیزات در قالب کارت های PCMCIA کـه در محـل مخـصوص خود نصب می شوند و یا به صورت اتصال خارجی از طریق یک درگاه USB عرضه می شوند.

برای رایانه ها رومیزی، می توانید از کارت های PCI و یا درگاه USB برای این منظور استفاده کنید. پس از نصب این تجهیزات کاربر قادر است تا در مکان هایی که اینترنت به شکل بدون سیم ارائه می شود با داشتن یک اشتراک، از خدمات بهره گرفته و به شبکه متصل شود.

وای‌فای را به دستگاه خود اضافه کنید

اشاره

مجهز بودن یک PDA یا اسمارت‌فون به وای‌فای با گسترش روزافزون این فناوری یک امر ضروری به‌نظر می‌رسد. حال اگر شما هم مانند من دستگاهی داشته باشید که فاقد این فناوری باشد، چه کار می‌کنید؟ مسلماً اولین راه حل، خریدن یک PDA جدید است، اما راه‌های ارزان‌تری نیز برای این مشکل وجود دارد. یکی از این راه‌ها افزودن سیستم وای‌فای به صورت خارجی به دستگاه می‌باشد. در ادامه نگاهی به این روش می‌اندازیم و کارت وای‌فای شرکت Spectec را بررسی می‌کنیم.

اکثر دستگاه‌های PDA امروزی از درگاه‌های حافظه استفاده می‌کنند و بسیاری نیز دارای دو درگاه حافظه هستند. در اکثر دستگاه‌ها این دو درگاه از نوع SD (Secure Digital) و CF (Compact Flash) هستند. اگر دستگاهی نیز دارای یک درگاه حافظه باشد، آن درگاه از نوع SD می‌باشد. البته استثنای این مسئله شرکت سونی می‌باشد که از کارت‌های حافظه خاص خود، یعنی stick memory استفاده می‌کند. در اکثر تجهیزات همراه

از جمله اسمارت فون‌ها امروزه از کارت‌های حافظه SD و نوع کوچک شده آن Mini SD استفاده می‌شود.کارت حافظه باعث افزایش توانایی ذخیره اطلاعات شده و بدون آن نمی‌توان به موسیقی گوش داد یا به فیلمی نگاه کرد؛ چرا ؟

که در اکثر دستگاه‌ها مقدار حافظه داخلی برای این کار کافی نیست. در حال حاضر حداکثر ظرفیت کارت حافظه SD چهارگیگابایت و کارت SD mini دوگیگابایت می‌باشد. این محدودیت ظرفیت در کارت CF کمتر بوده و حداکثر ظرفیت این نوع کارت ۳۲ گیگابایت می‌باشد.از این درگاه‌ها برای کاربردهای دیگری نیز استفاده می‌شود. به‌طور مثال، برای درگاه CF انواع مختلف دوربین، وای‌فای، بلوتوث و GPS ساخته شده است که قیمت‌های مناسبی نیز دارند.

حال اگر درگاه SD از فناوری SDIO (Secure Digital Input /Output) پشتیبانی کند، از این درگاه نیز می‌توان برای وسایل جانبی بهره برد. علاوه بر وسایل جانبی نامبرده، اسکنر بارکد و گیرنده امواج تلویزیونی نیز برای این درگاه طراحی شده است.البته استفاده از این وسایل به این راحتی نیست. این وسایل به نسبت وسایل جانبی درگاه CF گران‌تر بوده و در بازار به راحتی پیدا نمی‌شوند. در ضمن اگر یک Pocket PC داشته باشید که فقط یک درگاه SD دارد، چه می‌کنید؟ کارت‌های جدیدی به بازار آمده‌اند که دو کار را با هم انجام می‌دهند. مثلاً هم بلوتوث هستند و درضمن ۲۵۶ مگابایت حافظه فلاش نیز دارند. همان‌طور که می‌دانید کارت‌های mini SD نمونه کوچک شده کارت‌های SD هستند. این فناوری نیز از SDIO پشتیبانی می‌کند. البته محصولات این گروه به علت اندازه کوچک بسیار کم هستند. SDW-۸۲۲ یک کارت mini SD می‌باشد که وای‌فای را به دستگاه شما می‌افزاید. تولیدکنندگان PocketPc، اسمارت‌فون و Communicator امروزه بیشتر به کارت mini SD علاقمند شده‌اند و علت این علاقه، استفاده بهینه از فضا در داخل دستگاه می‌باشد.این کارت برای دستگاهی مانند HP hw ۶۵۱۵ که فاقد وای‌فای می‌باشد، بسیار مناسب است. نصب کارت بسیار ساده است .

کافی است. آن را به جای کارت حافظه وارد کنید و راه‌انداز را نصب کنید. بعد از آن نرم‌افزار داخلی ویندوز موبایل کارت وای‌فای را می‌شناسد و با آن کار می‌کند. با این‌که آنتن این کارت در حد چند میلی‌متر است، کیفیت سیگنال بسیار خوب است. این کارت از استاندارد b۸۰۲,۱۱ استفاده می‌کند و در اکثر اوقات ارتباط مناسبی برقرار می‌کند.

مهندسان سازنده این کارت تلاش زیادی کرده‌اند تا تمام اجزای یک سیستم وای‌فای را در فضای اندکی بزرگ‌تر از یک سیستم کارت موبایل جا بدهند. قیمت کارت در بازار جهانی در حدود صد و ده دلار می‌باشد و با توجه به این‌که وای‌فای گزینه مطلوبی برای بسیاری از کاربران است، قیمت این کارت مناسب به نظر می‌رسد.

مشخصات

مدل: SDW-۸۲۲ پروتکل ارتباطی: IEEE ۸۰۲,۱۱b سرعت: ۱۱Mbps/۵,۵Mbps پروتکل‌های امنیتی: PA و WEP ابعاد: ۱۰٤*۲۸*۲۰وزن; ۱,۵gr

به شبکه های WiFi باز وصل نشوید

مطمئن شوید که تنظیمات سیستم به گونه‌ای است که مانع اتصال خودکار به نقاط دسترسی ناامن شود.

اتصال به یک شبکه WiFi باز مثل یک hotspot یا مسیریاب بی‌سیم آزاد، کامپیوتر شما را در معرض خطرات فراوانی قرار می دهد. هرچند به طور معمول این امکان فعال نیست ولی اغلب کامپیوترها دارای تنظیماتی هستند که امکان اتصال خودکار بدون اطلاع کاربر را فراهم می‌کنند. این تنظیمات به‌جز در موارد ضروری و به‌طور موقت نباید فعال باشد.

برای بررسی این‌که آیا اتصال خودکار به شبکه‌های WiFi باز، مجاز است یا نه، تنظیمات بی‌سیم کامپیوتر را بررسی کنید. برای مثال در کامپیوترهایی که دارای Windows XP هستند، تنظیمات بی‌سیم Automatically connect to non-preferred networks نامیده می‌شود.

برای بررسی مراحل زیر را انجام دهید:

- از منوی start به گزینه Windows Control Panel بروید.
- به گزینه Network Connections بروید
- بـر روی Wireless Network Connection کلیـک راسـت کنیـد و گزینـه Properties را انتخاب کنید.
- روی گزینه Wireless Networks کلیک کنید.
- بر روی دکمه Advanced کلیک کنید.
- گزینـه Automatically connect to non-preferred networks را پیـدا کنیـد، اگـر انتخاب شده بود این تنظیمات فعال است در غیر این صورت غیرفعال است.

اگرچـه در Windows XP بـه‌طـور پـیش فـرض Automatically connect to non-preferred networks فعال نیست، برخی کاربران برای سهولت اتصال به شبکه خودشان آن را فعال می‌کنند. کـاربران بایـد

شبکه خودشان را به عنوان Windows XP Preferred networks تنظیم کنند که اجازه اتـصال خودکـار را می‌دهد و اتصال خودکار به بقیه شبکه‌ها را غیرفعال کنند.

۷. به تجهیزات آدرس (IP) ایستا اختصاص دهید.

اختصاص آدرس ایستا جایگزینی برای پروتکل DHCP است. اختصاص آدرس پویا با استفاده از DHCP راحـت تر است و هم چنین به کامپیوترهای سیار اجازه می دهد که بین شبکه های مختلف جابه جا شوند.

آدرس دهی ایستا نیز مزایایی دارد، از جمله:

- آدرس ثابت ترجمه آدرس را بهتر پشتیبانی می کند، بنابراین یک کامپیوتر روی شبکه با نام دامنه اش به طور مطمئن قابل دستیابی است. مخصوصا سرورهایی مثل سرور وب و سرور FTP بهتر است آدرس ایستا داشته باشند.
- استفاده از آدرس دهی ایستا در مقابل DHCP محافظت بیشتری در برابر حملات امنیتی فراهم می کند.
- برخی تجهیزات شبکه پروتکل DHCP را پشتیبانی نمی کنند.
- استفاده از آدرس دهی ایستا برای تمام اجزای شبکه تضمین می کند که ناسازگاری آدرس ها رخ نمی دهد.

آدرس های ایستا باید از محدوده آدرس های خصوصی استاندارد انتخاب شود از جمله:

- "۱۰,۰,۰,۰" تا "۱۰,۲۵۵,۲۵۵,۲۵۵"
- "۱۷۲,۱۶,۰,۰" تا "۱۷۲,۳۱,۲۵۵,۲۵۵"
- "۱۹۲,۱۶۸,۰,۰" تا "۱۹۲,۱۶۸,۲۵۵,۲۵۵"

این محدوده ها تعداد زیادی آدرس را پشتیبانی می کنند. برخلاف تصور اکثر افراد، تمام آدرس های این محدوده ها نمی توانند انتخاب شوند.

برای انتخاب آدرس درست نکات زیر را مدنظر داشته باشد:

۱. آدرس هایی که با "۰" یا "۲۵۵" تمام می شوند را انتخاب نکنید. این آدرس ها برا ی استفاده پروتکل های شبکه رزرو شده اند.

۲. آدرس های ابتدای یک محدود آدرس خصوصی را انتخاب نکنید. آدرس هایی مثل "۱۰,۰,۰,۱" یا "۱۹۲,۱۶۸,۰,۱" معمولا به مسیریاب ها ی شبکه اختصاص می یابند. این آدرس ها اولین آدرس هایی هستند که معمولا یک نفوذگر تلاش می کند به آن ها نفوذ کند، بنابراین بهتر است از آن ها استفاده نکنید.

۳. از آدرس هایی که خارج از محدوده mask شبکه شما می باشد استفاده نکنید. برای مثال، برای پشتیبانی تمام آدرس های محدوده "۱۰.x.x.x"، mask شبکه برای تمام سیستم ها باید به "۲۵۵,۰,۰,۰" تنظیم شود، در غیراین صورت برخی آدرس های ایستای این محدوده کار نمی کنند.

۸. قابلیت فایروال را روی تمام کامپیوترها و مسیریاب‌ها فعال کنید

یکی از آسان ترین و ارزان ترین راه ها برای محافظت از شبکه در برابر حملات استفاده از فایروال شخصی است.

۹. مسیریاب‌ها و نقاط دسترسی را در مکان‌های امن قرار دهید

کارآیی شبکه Wi-Fi به میزان زیادی بستگی به قدرت سیگنال مسیریاب یا نقطه دسترسی بی سیم دارد. اگر یک client بی سیم خارج از محدوده قدرت سیگنال قرار بگیرد ارتباط آن با شبکه قطع می شود یا ارتباط بسیار ضعیف می‌باشد. Clientهای بی سیم واقع شده در لبه شبکه ممکن است به دفعات زیاد ارتباطشان قطع شود، ولی حتی زمانی که یک Client بی سیم در محدوده قدرت سیگنال هم باشد، کارآیی شبکه از مواردی همچون فاصله، انسداد، یا تداخل تاثیر می گیرد.

برای تعیین محل قرار گرفتن تجهیزات بی سیم نکات زیر را مدنظر داشته باشد:

❖ اولین و مهم ترین نکته این است که، از قبل جایی را برای مسیریاب یا نقطه دسترسی بی سیم در نظر نگیرید. سعی کنید تجهیزات را در چندین نقطه متفاوت امتحان کنید. با وجود این که روش آزمون و خطا

راهکار علمی برای یافتن محل قرارگیری تجهیزات بی سیم نیست اما از دیدگاه عملی بهترین روش برای به دست آوردن حداکثر کارآیی است.

- سعی کنید مسیریاب یا نقطه دسترسی بی سیم را نزدیک به مرکز قرار دهید. Clientهایی که از ایستگاه مرکزی فاصله بیشتری دارند، در مقایسه با Clientهایی که نزدیک ایستگاه مرکزی هستند ، فقط از ۱۰ تا ۵۰ درصد پهنای باند بهره مند می شوند.

- تا حدامکان سعی کنید از موانع فیزیکی دوری کنید. هرگونه مانعی در فاصله خط دید بین Client و ایستگاه مرکزی باعث کاهش قدرت سیگنال می شود. دیوارهای آجری، خشتی، یا ساروج اندود بیش ترین تاثیر منفی را دارند ولی موانع دیگر نیز باعث کاهش قدرت سیگنال می شوند.

- تا حد امکان از سطوح بازتابی اجتناب کنید. برخی سطوح بازتابی مثل پنجره ها، آینه ها و ... باعث کاهش محدوده قدرت سیگنال های WiFi و در نتیجه کارآیی شبکه می شود.

- مسیریاب یا نقطه دسترسی بی سیم را حداقل به فاصله یک متر از دیگر تجهیزاتی که در محدوده فرکانس مشابه سیگنال بی سیم می فرستند قرار دهید. این ابزارها می تواند شامل تلفن بی سیم، اجاق های مایکروویو و ... باشد.

- همچنین مسیریاب یا نقطه دسترسی بی سیم را دور از تجهیزات الکتریکی که باعث ایجاد تداخل می شوند قرار دهید.

- اگر مکان مناسبی که پیدا کردید فقط به طور مرزی قابل قبول شود، آنتن های ایستگاه مرکزی را برای بهبود کارآیی تنظیم کنید. می توانید آنتن های مسیریاب و نقاط دسترسی بی سیم را بچرخانید و محل آن را تغییر دهید، دستورالعمل های کارخانه سازنده را اعمال کنید تا بهترین کارآیی را به دست آورید.

اگر با استفاده از این نکات و دستورالعمل ها باز هم مشکل دارید، می توانید به عنوان مثال آنتن های خود را تغییر دهید، یک تکرارکننده نصب کنید، یا در مواردی ایستگاه مرکزی دیگری پیکربندی و استفاده کنید.

۱۰. در فواصل زمانی طولانی که از شبکه استفاده نمی‌کنید تجهیزات را خاموش کنید.

اغلب ارتباطات اینترنت باندپهن همیشه برخط هستند. به همین خاطر دارندگان شبکه ترجیح می دهند اکثر تجهیزات شبکه مثل مسیریاب یا مودم روشن بماند حتی اگر برای مدت های طولانی بدون استفاده باشند.

ولی آیا شبکه های محلی هم لازم است همیشه روشن بمانند؟ خاموش کردن تجهیزات شبکه چه مزایا و معایبی دارد؟

در ادامه برخی از مزایا و معایب خاموش کردن تجهیزات شبکه را هنگامی که استفاده ای از آن ها نمی شود، بررسی می کنیم:

امنیت: خاموش کردن تجهیزات شبکه زمانی که در حال استفاده نیستند، باعث افزایش امنیت شبکه می شود. زمانی که تجهیزات شبکه خاموش باشند نفوذگران قادر به انجام کاری نیستند.

صرفه جویی در مصرف برق: خاموش کردن تجهیزات شبکه باعث صرفه جویی در هزینه ها می شود. در برخی کشورها این صرفه جویی چندان قابل توجه نیست اما در برخی کشورها نیز به علت بالا بودن هزینه انرژی میزان قابل توجهی است.

محافظت در برابر اعوجاج سیگنال: جدا کردن تجهیزات شبکه باعث جلوگیری از خرابی های احتمالی منتج از اعوجاج سیگنال می شود. ممکن است گفته شود که محافظ ها هم قادرند از ابزارها در برابر اعوجاج مراقبت کنند ولی این محافظ ها به خصوص انواع ارزان قیمت آن قادر به مراقبت در برابر نوسانات شدید نیستند.

قابلیت اطمینان سخت افزار: قطع و وصل مدام منبع انرژی تجهیزات شبکه باعث کاهش طول عمر آن ها می شود. دیسک درایوها اغلب آسیب پذیر هستند. به عبارت دیگر، دمای زیاد هم باعث کاهش طول همه ابزارهای شبکه می شود. همیشه روشن گذاشتن تجهیزات شبکه در مقایسه با زمانی که تجهیزات گهگاه خاموش می شوند، احتمالا باعث آسیب های بیش تری می شود.

قابلیت اطمینان ارتباطات: بعد از خاموش و روشن کردن تجهیزات ممکن است فرآیند برقراری ارتباط مجدد با خطا مواجه شود. باید فرآیند راه اندازی مجدد را با احتیاط دنبال کنید. به عنوان مثال باید ابتدا مودم های باندپهن

روشن شوند و ابزارهای دیگر پس از این که مودم آماده شد، روشن شوند. همچنین اگر هنگام راه اندازی یا نـصب با خطایی مواجه می شوید حتما راه حلی برای آن پیدا کنید در غیـراین صـورت ممکـن اسـت در آینـده منجـر بـه مشکلات بزرگ تری شود.

سهولت: تجهیزات شبکه مثل مسیریاب بی سیم یا مودم ممکن است در مکان هایی مثل سقف یا مکـان هـایی کـه دسترسی به آن ها سخت است قرار داشته باشد. هنگام خاموش کردن این تجهیزات احتیاط نموده و به جای استفاده از دکمه خاموش و روشن کردن تجهیزات، رویه های توصیه شده توسط کارخانه سازنده را حتما رعایت کنید.

به طور خلاصه با درنظر گرفتن ملاحظات فوق الذکر پیشنهاد می شود که در زمان هایی که از شـبکه اسـتفاده نمـی کنید تجهیزات را خاموش کنید. مزایای امنیتی آن به تنهایی کافی است تا این کار را انجام دهیم.

آگاهی و درک ریسک ها و خطرات WIFI

وقتی شما مشغول یافتن ابزار WIFI هستید ابتدا باید از ریسک ها و خطراتی که زیر ساختار شما را تهدییـد مـی کنند آگاه شوید .یکی از بدهی ترین ریسک ها تهدید ترافیک خود شبکه بی سیم است. یک مهـاجم ممکـن اسـت بهsniffing شبکه شما دسترسی به شبکه شما یا حتی تغییر داده هایی که از طریق شبکه منتقـل مـی شـوند علاقـه داشته باشد. اگر شما دارای نقاط دسترسی باشید که به هر دلیلس رمز گـذاری نـشده باشـد sniffing ترافیـک یـا دسترسی به شبکه ها یک فعالیت کم اهمیت و جزئی به شمار می رود .اما حتـی بـرای شـبکه هـایی کـه بـا wep رمزگذلزی شده اند نیز مانعی که برای جلوگیری از دسترسی فرد مهاجم وجود دارد یک مانع نـسبتا ضـعیف اسـت .وقتی مشغول بررسی و ارزیابی یک شبکه هستید باید نگران شبکه های رمز نگـاری نـشده یـا شـبکه هـایی کـه از رمزگذاری ضعیف استفاده می کنند باشید.خوشبختانه عمر wifi در شربت هایی با سایز معقول به انـدا زه ای بـوده است که تعداد نقاط دسترسی محافظت نشده در انها به حداقل ممکن برسد.هرچند شبکه های خانگیو دفتـری یـک موضوع کاملا متفاوت هستند.انها هنز هم کاملا بلادفاع هستند.یکی دیگر از ریسک هایی که شبکه شما با آن مواجه است نقاط دسترسی rouge است که به شبکه های با سیم شما متصل میشود.و یکی از بزرگ ترسن ریـسک هـای پیش روی شبکه های wifi مدرن خو خدمات گیرنده های بیسیم هستند .حتی اگر شبکه شـما بـه شـکلی صـحیح

پیکربندی شده باشد خدمات گیرنده شما می توانهد همه چیز را خراب کنند.به جای حمله مستقیم به شبکه یک مهاجم ممکن است یکی از خدمات گیرنده ها را بای دسترسی به بقیه ترافیک موجود بر روی شبکه انتخاب کند.

یکی از روش های متداول و رایج انجام این هدف پیدا کردن خدمات گیرنده هایی است که در حال بررسی سایر شبکه ها هستند.به عنوان مثال بعضی از سیستم عامل ها (نظیر windows xp و os x) وقتی برای اولین با آن لاین می شوند یا وقتی ارتباط خود را باشبکه های قبلی که سیستم عامل به آن متصل شده بود از دست می دهند به طور اتوماتیک به دنبال یک شبکه بی سیم شناخته شده دیگر می گردند.وقتی قتی میزبان به دنبال یک شبکه می گردد یک probe packet رابا نام شبکه ای که سعی در پیدا کردن آن دارد ارسال می کند.یک مهاجم (و همچنین یک کاربر) می تواند برای مشخص کردن این که خدمات گیرنده به کدام شبکه ها اطمینان دارد بو بکشد(sniff کند) .مهاجم سپس می تواند یک نقطه دسترسی rogue که تظاهر می کند یکی از شبکه های مورد اطمینان است را ایجاد کند و سعی نماید خدمات گیرنده را مجبور کند به rogue جدید متصل شود .اگر مهاجم موفق شود خدمات گیرنده را فریب دهد.از یک اتصال سطح I P به خدمات گیرنده بر خوردار خواهد شد و می تواند با استفاده از آسیب پذیری های شناخته شده به میزبان دسترسی پیدا کند و در کار آن اختلال ایجاد نماید.وقتی مهاجم سیستم سیستم عامل را دستکاری کرد به طور کانل به سیستم داده هایی آن

و شبکه هایی که به آن متصل هستند دسترسی پیدا میکند.وضعیت خوبی نیست بنابراین توجه بیشتری به خدمات گیرنده های خود نشان دهید.

قبل از اینکه به دنبال ابزار بیسم بگردید زرادخانه خود را گرد آوری کنید.شما به یک کارت شبکه بی سیم مناسب و یک نرم افزار بیسیم و آنتن نیاز خواهید داشت.

نرم افزار

انتخاب کارت ها و نرم افزارها ممکن است در هماهنگی با هم صورت بگیرد .بعضی از نرم افزار ها برای کارکرد به نوع خاصی کارت نیاز دارند .به عنوان مثال AirSnort یک ابزار رایج و متذژداول برای لینوکس (و نسخه های BSD) است که ابزار بیسیم را پیدا می کند و به WEP حمله می کند .هرچندAirSnort برای این که قادر به کار باشد به یک کارت بیسیم با چیپ ست Prism ll نیاز دارد. در سایت وب AirSnort به این نوع کارت های خاص و چگونگی استفاده از آنها اشاره شده است.

NetStumbler یک ابزار محبوب برای استفاده در ویندوز است که از مدت ها قبل در دسترس قرار داشته است.هر چندارای نقاط ضعفی به شرح زیر می باشد:

- NetStumbler خدمات گیرنده ها را کشف نمی کند بلکه فقط نقاط دسترسی را تشخیص می دهد .اگر شما شما به دنبال خدمات گیرنده ها می باشید NetStumbler ابزار مناسبی برای کار شما نیست.
- NetStumbler فقط نقاط دسترسی را که beacon ها را ارسال می کنند می بیند.نقاط دسترسی که از طریق عدم ارسال beacon خود را پنهان می کنند توسط NetStumbler تشخیص داده نمی شوند.
- NetStumbler پر سر و صدا یا loud است زیرا به منظور کوشش برای یافتن نقاط دسترسی بی سیم بسته های متعددی ارسال می کند.اگر شما به پنهان سازی و پنهان کاری علاقه دارید از NetStumbler استفاده نکنید.

Kismet یک ابزار عالی است که بر روی سیستم های لینوکس و BSD ها اجرا می شود.Kismet بر خلاف NetStumbler یک ابزار گرافیکی نیست اما قادر است خدمات گیرنده ها راو نقاط دسترسی cloak شده را تشخیص دهدو با انواع گوناگون و متعددی از کارتها نظیر کارت های Cisco و بسیاری از کارت هایی که در اکثر فروشگاهای لوازم الکترونیکی عرضه می شوند کار می کند.Kismet می تواند داده های خود را در فرمت های گوناگونی ذخیره کند که چنانچه شما باdataset های بزرگ سروکار داشته باشیدبرایتان بسیار مفید خواهد بود.بای کاربران دنیای OS X نیز KisMAC وجود دارد. KisMAC این است که وقتی برای استفاده از اینترفیس بی سیم AirPort Extrcmc کمپانی Apple پیکر بندی شود قادر به دیدن خدمات گیرنده ها و نقاط دسترسی cloak شده نیست.به منظور فراهم شدن امکان استفاده از تمام قابلیت های KisMAC به کارت third-parry نیاز خواهید داشت.در عین گستره گوناگونی از ابزار تجاری نیز وجود دارد که شما می توانید از آنها استفاده کنید.AiroPeek ساخت کمپانی Wild Packetیک ابزار محبوب و پر طرفدار برای کشف ابزار بی سیم است .استفاده ازAiroPeek آسان است و در کمپانی های بزرگ به خوبی عمل می کند.این نرم افزار امارها و نمدارهایی تولید می کند که خواندن آنها بسیار آسان است و به شما اجازه می دهد تغییرات ایجاد شده در کمپانی خود را در طی زمان به راحتی مشاهده کنید.

تنظیم درست و صحیح تمامی متغییر ها برای بر قراری ارتباط کارت ها و نرم افزار با هم می تواند کار مشکلی باشد. یکی از بهترین روش ها برای تجربه با ابزاری نظیر Kismet و AirSnort با سی دی قابل بوت Auditor از Remote-Exploit.orgاست.Auditor یک توزیع قابل بوت کامل لینوکس با چندین ابزار امنیتی در داخل آن است که دارای مجموعه وسیعی از اسکریپ هایی است که نرم افزار بی سیم و کارت ها را به منظور کار اتوماتیک.autoconfigure (پیکربندی اتوماتیک) می کند..به عنوان مثال اگر بخواهیدAirSnort را امتحان کنید اما نخواهید وارد وادی خسته کننده پیکربندی همه چیز به گونه ای که به خوبی با هم کار کنند بشوید. Auditorبهترین ابزاری است که می تواند به شما کمک کند.

سخت افزار

شما ممکن است به آنتن ها نیاز داشته باشید یا نیاز نداشته باشید که این امر به موقغیت وضعیتی که در آن هستید بستگی دارد.به طور خلاصه باید گفت که آنتن ها سیگنال های ارسالی و دریافتی شما را تقویت می کنند. اگر در داخل یک ساختمان roaming می کنید.ممکن است به آنتن نیاز نداشته باشید هر چند اگر در یک مجموعه بزرگتر کار می کنید یا قصد دارید یک ناحیه وسیع تر را به سرعت تحت پوشش قرار دهید احتمالا باید از آنتن استفاده کنید.آنتن ها دو نوع هستند:

- آنتن های چند جهته (omnidirectional) سیگنال های ۳۶۰ درجه ای را در اطراف محور آنتن تقویت می کنند.
- آنتن های یک جهته(dircctional) سیگنال ها را در یک bcam باریکتر تقویت می کنند.

قدرت یک آنتن با دسی بل (db)اندازه گیری می شود که هرچه بزرگتر باشد قدرت آنتن بیشتر خواهد بود.هرچند مراقب باشید زیرا یک آنتن قویتر دارای سیگنال های فوکوس شده بیشتری است که ممکن است کار یافتن ابزار بی سیم را مشکل تر کند.به طور کلی یک آنتن omnidirectionul(چند جهته) بای کشف ابزار بی سیم کفایت میکند.ضمنا فراموش نکنید کابلی را که برای اتصال آنتن به کارت ساخته شده است را تهیه نمایید.

استفاده از تکنولوژی MIMO جهت افزایش سرعت WiFi زیر دریا

همچنانکه ایالات متحده و کانادا اولین قدم های خود را به سوی تاسیس یک رصدخانه اقیانوسی کابل کشی شده بر می دارند، یک محقق دانشگاه میسوری رولا در تلاش برای بهبود سرعت ارتباطات زیر آبی بی سیم می باشد. به گفته دکتر رزا ژنگ، استادیار دانشکده مهندسی برق و کامپیوتر UMR، همان امواج اکوستیکی که دلفین ها و وال ها برای ارتباط استفاده می کنند در حالی که هزاران مایل از یکدیگر فاصله دارند، می تواند توسط انسان ها برای ارسال اطلاعات بصورت بی سیم استفاده شود. تمرکز تحقیق این دانشمند بر روی ارتباطات درون آب های کم عمق می باشد که برای دیده بانی محیطی و دیگر موارد مورد نیاز است. ارتباطات آب های کم عمق با چالش های افزوده ای مواجه است چرا که سیگنال ها بوسیله امواج و پژواک کنار صفحات زیرین و فوقانی اقیانوس تحت تاثیر قرار می گیرند.

خانم رزا ژنگ اضافه کرد: "نکته ی شگفت انگیز در مورد سیگنال های اکوستیک این است که هر چه فرکانس پائین تر باشد، فاصله بیشتری را می تواند طی کند. نقطه ی چالش انگیز اینجاست که امواج اکوستیک پهنای باند بسیار محدودی دارند. هدف ما این است که به یک سطح اطمینان بالا و نیز سعت انتقال داده بالا دست یابیم."

سرعت انتقال داده در سیستم های کنونی ارتباطات زیر دریایی، معمولا محدود به چند کیلوبیت بر ثانیه می باشد، که بسیا پائینتر از سرعت مگابیت بر ثانیه ای است که توسط ارتباطات بی سیم RF (فرکانس های رادیوئی) ارائه می شود. این استاد دانشگاه، قصد دارد تا از تکنولوژی چند–ورودی، چند–خروجی (MIMO) – تکنیکی که چند مسیر و آنتن را اهرم می کند – به منظور افزایش سرعت انتقال داده تا چندصد کیلوبیت بر ثانیه استفاده کند.

ژنگ همچنین افزود: "تکنولوژی MIMO چند چالش برای ما بوجود خواهد آورد چرا که شما سیگنال ها را در یک زمان و بوسیله یک باند فرکانسی ارسال می کنید. به لحاظ تئوری اثبات می شود که اینکار امکان پذیر است اما ما هنوز در تلاش هستیم تا ببینیم چگونه می توان آن سیگنال ها را در دریافت کننده از یکدیگر جدا کرد."

ژنگ و دانشگاه میسوری کلمبیا، برای سرمایه گذاری بر روی این طرح یک مقرری ۲۷۰ هزار دلاری به مدت سه سال از طرف Naval Research دریافت کرده اند.

۵– محصولات WIFI

۵-۱این تل قرار است چیپ‌ست **Wi-Fi tri-mode** بسازد

۵-۲قاب عکس وای‌فای

۵-۳بررسی مادربرد جدید **ASUS** مدل**P۵E۳ Deluxe/Wifi**

۵-٤تراشه‌هایی با قابلیت ریزموج برای ارتباطات بی سیم

مقدمه :

امروزه استفاده از تکنولوژی Wi-Fiباعث شده که تمام شرکت های بزرگ سرمایه گـذاری هـای بزرگـی بـر روی تکنولوژی Wi-Fi انجام دهند و محصولاتی را با استفاده از این تکنولوژی ارائه دهند . عبارتند از :

اینتل قرار است چیپست Wi-Fi tri-mode بسازد

شرکت اینتل در راستای تحقق یک هدف دراز مدت قرار است اولین چیپست خود را معرفـی کنـد، کـه هـر سـه حالت رایج Wi-Fi پـشتیبانی مـی کنـد .بـه گـزارش بخـش خبـر سـایت اخبـار فـن آوری اطلاعـات ایـران، از PCWorldIran، با این چیپست کـه شـامل تکنولـوژی IEEE ۸۰۲,۱۱a/b/g اسـت، یـک کـامپیوتر شخـصی نوت‌بوک می‌تواند اتصال خود به انواع LAN بی‌سیم شرکت را بدون ارتقا و سـخت‌افـزار ادامـه دهـد، حتـی اگـر شرکت زیرساختار خود را تغییر دهد .

سازندگان دیگر نیز قبل از اینتل انواع چیپست تحت عنوان tri-mode را سـاخته بودنـد. در اوایـل سـال جـاری شرکت اینتل پیکربندی چیپست نوع ۸۰۲,۱۱ b/gرا معرفی کرد، اما قرار است شـرکت، سـه تکنولـوژی دیگـر را معرفی کندAmy Martin ،. سخنگوی اینتل از اظهار نظر در این مورد خودداری کرد، اما شرکت دعوت نامـه‌ای الکترونیکی منتشر کرد که معرفی جدیدترین تکنولـوژی بـی سـیم مخـصوص نـوت‌بوکهـای Centrino را اعـلام می‌نمودMike Feibus ،. یکی از تحلیلگران در Techknowlege Strategies Inc در شهر اسکاتزدیل ایالـت آریزونا می‌گوید، این محصول حقیقتا دوران شکوفایی شرکت اینتل را به نمایش می‌گـذارد . البتـه وسـعت شـرکت اینتـل باعـث شـده اسـت کـه نـسبت بـه رقبـای کـوچکترش از جملـهAtheros Communications Inc ، Braadcom corpو Texas Instruments Inc سرعت رشد کمتری داشته باشد. این شرکتها چند ماهی است که انواع چیپست را در اختیار دارند. تحلیلگری به نام آقای Bob Wheeler در Linely Group می‌گویـد، در ضمن شرکت اینتل به دلیل سرمایه‌گذاری زیادی که در گروه Centrino کرده است بسیار محتاط عمل می‌کند. این شرکت تمامی محصولات خود را مورد آزمایشات دقیق و جدی قرار می‌دهد تا ابتدا از همـاهنگی و تطـابق آنهـا و

سپس از هماهنگی آنها با انواع مشخصه‌ها اطمینان حاصل کند . تکنولوژی‌های ۸۰۲,۱۱ bاز امواج رادیویی با طول موج ۲,٤ گیگاهرتز جهت انتقال اطلاعات با سرعت ۱۱ Mbpsاستفاده می‌کند و تکنولوژی ۸۰۲,۱۱g از امواج رادیویی یکسان برای انتقال اطلاعات با سرعت ٥٤ Mbps استفاده می کند. مدل غیر متداول‌تر ۸۰۲,۱۱ aنیز با طول موج ٥ گیگاهرتز برای ارسال اطلاعات با سرعت ٥٤ Mbps را نیز می‌توان در کانال‌های بیشتر به طور همزمان مورد استفاده قرار داد. به علاوه در طول موج ٥ گیگاهرتز تداخل کمتر نیز وجود دارد . تکنولوژی ٥ گیگاهرتز احتمالا بیش از دیگران مورد استقبال واقع می‌شود، زیرا شبکه‌های g و ۸۰۲,۱۱ با کاربران بیشتری انباشته می‌شوند و تکنولوژی‌های ۲,٤ گیگاهرتزی تنها امکان استفاده همزمان سه کانال را فراهم می‌آورند. اما تعداد کانال‌ها در ۸۰۲,۱۱ aدر کشورهای مختلف متفاوت است، اما عموما پیش از سه کانال است. این شبکه در آمریکا تا ۲٤ کانال را پشتیبانی می‌کند، که می‌تواند در ادارات، سالن‌های اجتماع بزرگ حقیقتا تغییرات بزرگی را سبب شود. برنامه جدید دیگر که با ۸۰۲,۱۱ aبه راه می‌افتد، سیستم‌های سرگرمی خانگی بی‌سیم است .

Will Straussاز تحلیلگران ارشد شرکت Forward Concepts Co در Tempe ایالت آریزونا می گوید: بازاریابی Centrino نیز که ساخت خود اینتل است، می‌تواند به تکنولوژی tri-mode کمک زیادی کند. البته او معتقد است که کاربران بخصوص مشتریان بیشتر از ۸۰۲,۱۱ b/gراضی خواهند بود. تقاضا برای ۸۰۲,۱۱a به طور ناگهانی افزایش نخواهد یافت Strauss .می‌گوید: قطعا تقاضا برای این محصول روز به روز بیشتر می شود، اما ...، مثل تقاضا برای چوب هاکی نخواهد بود . تحلیلگر دیگری می‌گوید Tri-mode :حداقل در بازار تجارت آینده درخشانی خواهد داشت Abner Germanow .در IDC در شهر فرامینگهام ایالت ماساچوست می‌گوید :بزودی محصولات اداری به بازار می‌آیند که تنها درa/b/g استفاده می‌کنند شاید تا سه ماهه اول یا دوم سال آینده اگر زودتر نباشد .

قاب عکس وای‌فای

اشاره :

شرکت‌های سازنده تجهیزات سخت‌افزاری به شدت به قاب عکس‌های دیجیتالی علاقمند شده‌اند و سعی دارنـد تـا دیر نشده است، گوی سبقت را از رقبا ببرند و بازار را تصرف کنند.

شرکت‌های سازنده تجهیزات سخت‌افزاری به شدت به قاب عکس‌های دیجیتالی علاقه‌مند شده‌اند و سعی دارند تـا دیر نشده است، گوی سبقت را از رقبا ببرند و بازار را تصرف کنند. سامسونگ نیز قاب عکس دیجیتالی خود با نـام SPF-۸۳V را معرفی کرد. این محصول که اولین قاب دیجیتالی سامسونگ است، مجهز به یک صفحه‌نمایش هشت ایـنچ و حافظـه ٦٤مگابـایتی اسـت.البتـه قابلیـت افـزودن کـارت‌هـای حافظـه CompactFlash، SD،xD و Memory Stick را نیز دارد. V۸۳ با یک پورت USB به کامپیوتر متصل می‌شود. اما کلید پیروزی سامسونگ در این محصول نسبت به رقبا در پوشش دادن فناوری وای‌فای است.V۸۳ از پروتکل g۸۰۲,۱۱ پشتیبانی می‌کنـد. ایـن قابلیت امکان تبادل تصویر را میان این محصول و دستگاه‌های دارای وای‌فای مانند گوشی تلفن همراه، نـوت‌بـوک، شبکه‌های بی‌سیم و حتی سایت‌های اشتراک عکس فراهم می‌کند.

بررسی مادربرد جدید ASUS مدلP۵E۳ Deluxe/Wifi

این مادربوردها بر مبنای چیپست X۳۸ Intel تولید شده است که عملکردی مناسب در بهینه‌سازی مـصرف انـرژی دارد. قابلیت پـشتیبانی از حافظـه۱۸۰۰ MHz ، DDR۳ دو کانالـه و Dual PCI Express ۰/۲ ١٦x lanes از دیگر ویژگی‌های این مادربورد به منظور افزایش کارایی است.برای اولین بـار در دنیـا در ایـن مـادربورد از EPU)واحد پردازش انرژی) استفاده شده است که امکان کنترل دیجیتالی مصرف انرژی توسط CPU را فراهم می‌کنـد و این امکان را می‌دهد تا با تنظیم و افزایش بازدهی VRM و همچنین باتوجه به حجم بارگذاری (loading) ذخیره

انرژی به بهینه‌ترین روش در راستای کمک به محیط زیست انجام شود. این مادربورد همچنین قابلیت پشتیبانی از wifi n ۱۱/۸۰۲و تمامی ویژگی‌های آن را به صورت Onboard دارا است و امکان تبادل سریع‌تر اطلاعات را فراهم می‌سازد. فناوری ASUS Express Gate نیز که یک راه‌انداز اختیاری برای سیستم عامل linux است و امکان دسترسی سریع را در زمانی کمتر از پنج ثانیه امکان‌پذیر می‌سازدکه در این مادربورد به کار رفته است .

EPUدر واقع یک قطعه سخت‌افزاری است که با استفاده ازIC های کنترل کننده قادر است تا انرژی را به میزان قابل توجهی ذخیره کند. این نسل جدید از چیپ خودکار ذخیره‌ساز انرژی با استفاده از فناوری Hybrid Power و همچنین افزایش کارآیی VRM در زمان‌های بارگذاری (Loading) قادر است تا به صورت دیجیتال میزان مصرف انرژی توسط CPU را تنظیم و کنترل کند. روش کار نیز بدین صورت است که این چیپ با انجام بازرسی سریع و لحظه به لحظه CPU قادر است تا یک شمای کلی از وضعیت بارگذاری CPU را به دست آورده و سپس بهترین و موثرترین روش‌های ذخیره‌سازی را به کار می‌برد تا علاوه بر کمک به حفظ محیط زیست به طور خودکار قدرت و کارایی بیش‌تر را فراهم آورده و در مواقعی که سیستم در حال اجرای برنامه‌های سبک است به میزان ٥٦/٦ درصد توان CPU را ذخیره می‌کند ASUS.با طراحی نسل سوم VRM هشت فاز تا ۹۵ درصد مصرف انرژی را در مقایسه با سایر روش‌ها بهینه می‌کند. طول عمر بیش‌تر قطعات و اتلاف انرژی کمتر، از جمله ویژگی‌های قطعات با کیفیت است که از آن جمله می‌توان به استفاده ASUS از MOSFET ها به منظور به حداقل رساندن میزان اتلاف انرژی و کم کردن حرارت با خازن‌های پلیمری ساخت ژاپن اشاره کرد ASUS Express Gate.یک راه‌انداز اختیاری است که امکان دسترسی سریع کاربر به اینترنت را بدون نیاز به وارد شدن به Windows می‌دهد. با استفاده از این امکان کاربران می‌توانند به راحتی از امکاناتی نظیرSKype ، IM، You Tubeو Webmail استفاده کنند.گفتنی است کاربران قادر خواهند بود باتوجه به پشتیبانی این مادربورد از فناوری IEEE ۱۱/۸۰۲ n به صورت Onboard از پوشش بیش‌تر شبکه و تبادل سریع‌تر داده تا شش برابر به نسبت استاندارد ۸۰۲ /۱۱ b/g نهایت

لذت را ببرند. همچنین با اتصال دو آنتن، حوزه پوشش‌دهی شبکه افزایش یافته و سیگنال‌ها به خوبی قادر خواهند بود از موانع پیش‌رو حتی دیوار نیز عبور کنند. بدین ترتیب کاربران می‌توانند در هر جایی و بدون وجود حتی یک نقطه کور آنلاین شوند.

تراشه‌هایی با قابلیت ریزموج برای ارتباطات بی سیم

یکی از پروژه‌های اخیر اتحادیه اروپا یک ریزتراشه نشانگر جدید را طراحی و تولید کرده است که به صورت چشمگیری هزینه‌ی تولید کالاهای بدون سیم را کاهش خواهد داد و این بدین معناست که طیف وسیعی از کالاهای موجود، قابلیت ارتباطات بدون سیم را پیدا خواهد کرد.

پروژه IMPACT که از طرف IST حمایت مالی می‌شود، شامل شرکت‌های غول‌پیکر صنعتی Ericsson و Philips می‌شود که برای ساخت تراشه‌ای که سیگنال‌های ریز موج را در بازه فرکانس ۵ تا ۲٤ گیگاهرتز بفرستد و دریافت کند، با هم کار می‌کنند. این تیم طیفی از نشانگرها شامل آمپلی‌فایرها، نوسانگرها، مخلوط‌کن‌ها و تقویت کننده‌های فرکانس را طراحی کرده است.

گروه IMPACT انتظار دارد، مدارهای آنالوگ و با فرکانس بالا کشف کند که با تراشه‌های CMOS ۹۰ نانومتری قابل تطبیق باشد. این تراشه‌ها از مدارهای بسیار کوچک‌تر (۹۰ نانومتر) از مدل‌های فعلی استفاده می‌کند.

دکتر استفان دکوتر، مسئول هماهنگی پروژه IMPACT و محقق مرکز بین دانشگاهی میکروالکترونیک بلژیک می‌گوید: تراشه‌ها دیجیتال CMOS و در اندازه‌های ۹۰ نانومتر، امسال (سال ۲۰۰۵) قابل دسترسی خواهند بود و می‌خواهیم بدانیم آیا می‌توانیم آنها را در ارتباطات ریزموجی با فرکانس بالا استفاده کنیم. تراشه‌های CMOS با فرکانس بالای قدیمی‌تر، از قبل در تجهیزات ۲/٤ گیگاهرتزی مانند فرستنده‌ها و گیرنده‌های بلوتوس که به طور جداگانه توسط Ericsson ، یکی از طرف‌های پروژه طراحی شده است، استفاده شده‌اند. ولی به گفته دکتر دکوتر، نیازهایی که برای استفاده از این تراشه‌ها در سطوح بالا و پیچیده چون GSM یا "سامانه جهانی ارتباطات سیار" وجود دارد، دست نیافتنی‌ترند. در حال حاضر این کاربردها احتیاج به راه‌حل‌های گران‌قیمت و چند تراشه‌ای دارد.

گروهIMPACT متوجه شده‌اند، تراشه‌های CMOS می‌توانند برطرف کننده نیازهای پیچیده و صعب‌الوصول لازم برای کاربردهای میان برد و پیشرفته‌ای چون GSM و ارتباطات ریزموجی نقطه به نقطه باشند. این تراشه‌ها به نحو قابل‌توجهی از هزینه‌ها و میزان مصرف انرژی خواهند کاست و بر کاربردهای این تجهیزات خواهند افزود.

به گفته دکتر دکوتر، ساخت این تراشه‌ها اکنون بسیار هزینه‌بر است، ولی با گذشت زمان بسیار ارزان‌تر خواهد شد. به دیل این که تمام مدارها بر روی یک تراشه قرار دارد، فرآیند تولید بسیار اثر بخش‌تر خواهد بود و تراشه‌های CMOS فرکانس بالا، در حجم وسیع و با هزینه‌های بسیار کمتر ساخته خواهد شد.

پتانسیل بالا

پتانسیل تراشه‌های CMOS در ارتباطات ریزموجی بسیار بالاست. به گفته پروفسور هربرت زیرات، یکی از اعضای IMPACT و استاد دانشگاه فناوری سوئد، CMOS می‌تواند در ارتباطات از راه دور و مدارهای راداری چون تلفن‌های همراه، شبکه‌های داخلی بی‌سیم (WLAN) و پیوندهایی سریع، که تعداد زیادی از کارکردها در آنها جمع شده‌اند، کاربرد داشته باشند. از آن جا که CMOS با تولید انبوه بسیار اقتصادی است و می‌تواند در کاهش هزینه‌ها بسیار مؤثر باشد.

تراشه‌های CMOS نوع مهمی از مدارهای مجتمع هستند که شامل میکروپردازشگرها، میکروکنترل‌کننده‌ها، حافظه‌های ایستا و دیگر مدارهای دیجیتال می‌شوند. این کارکردهای متفاوت می‌توانند در یک تراشه متمرکز شوند که علاوه بر کاهش هزینه‌ها، پیچیدگی تجهیزاتی چون دوربین‌های دیجیتال را کاهش خواهد داد.

تراشه‌های CMOS تنها زمانی که ترانزیستورهایشان خاموش و روشن می‌شوند، انرژی مصرف می‌کنند. بنابراین انرژی کمتری مصرف می‌شود و دمای کمتری نسبت به تراشه‌های عادی تولید می‌شود که این برای ارتباطات از راه دور ایده‌آل است.

به جلو راندن خط مقدم فناوری

گروه IMPACT ، دو موفقیت مهم به ثبت رسانیده است. نخست آن که آن‌ها به خصوصیات عملکردی مورد نظر در قیمت پایین‌تر و سطح پایین‌تری از مصرف انرژی دست یافته‌اند که با فناوری‌های موجود قابل دسترسی می‌باشد، سپس این که آنها از آخرین خط فناوری مدارها با فناوری CMOS فرکانس بالا و آمپلی‌فایرهای با

نشانگرهای دقیق و نوسانگرهای با ولتاژ کنترل شده که از لحاظ عملکرد دارای رکورد جهانی هستند، گذشته‌اند. پروژه، حمایت مشتاقانه طرف‌های صنعتی را به دست آورده است.

اریکسون اظهار می‌کند، پروژه به چشم‌انداز راهبردی خود برای استفاده از طیف فرکانس‌های ریزموجی دست یافته است و مزیت اصلی این پروژه در این نکته بوده است که با کاربردهای مشخص شروع شده است. پروژه حتی ممکن است برای کتاب سال تحقیقات ۲۰۰۵ اتحادیه اروپا، که تحقیقات برتر را بازتاب می‌دهد، انتخاب شود.

فناوری CMOS، در اندازهٔ ۹۰ نانومتری هم‌اکنون مورد استفاده است. به طور مثال کاربردهایی که اریکسون برای سه سال آینده از این فناوری در نظر گرفته است شامل ساماندهی شبکه‌های داخلی بی‌سیم چون WiFi و نقاط اتصال به جریان در بازه فرکانس ۵ تا ٦ گیگاهرتز است.

شرکت Philips ، طرف دیگر پروژه، کاربرد اصلی فناوری CMOS را ایجاد راه حل‌های اقتصادی و تأثیرگذار بر قیمت، برای ارتباطات بی‌سیم که یک بازار نوظهور مهم و با کاربردها و محصولات بالقوه فراوان است، می‌داند.

Philips اعتقاد دارد، این فناوری امکان بی‌سیم شدن را برای وسائل الکترونیکی فراهم خواهد آورد و تمام محصولات تمام الکترونیکی امکان بی‌سیم شدن و در نتیجه، تعاملات دستگاه با دستگاه را خواهند داشت.

این مسأله تنها تولیدات سطح بالا و تجملی را در بر نخواهد گرفت، بلکه می‌تواند تولیدات سطح پایین‌تری چون واکمن‌ها و MP۳ Playerها را در برگیرد.

البته چنین تجهیزاتی شدیداً به یکپارچه‌کردن فناوری فرکانس بالا و کارکردهای آنالوگ با فناوری CMOS در زمان معین و با هدف یافتن راه‌حل‌های اقتصادی و سامانه‌روی‌تراشه وابسته است که البته IMPCAT مسیر طولانی از این راه را پیموده است.

در زمان مناسب، IMPCAT قصد راه‌اندازی یک پروژه‌ی تکمیلی دارد که در صورت امکان تراشه‌های CMOS را با فرآیندهای در اندازهٔ ٤٥ نانومتر تولید کند.

دکتر دکوتر می‌گوید: اگر به اندازهٔ CMOS دیجیتال نگاه کنید. خواهید دید که تا حدود ٦٥ نانومتر همـان رویکـرد مربوط به تراشه‌های قبلی به کار گرفته می‌شود. اما در قطع ٤٥ نانومتر و پایین‌تر تقریباً مواد جدید و چینش جدیدی از آن‌ها مطرح است که ما در حال کشف آن هستیم. ما می‌خواهیم ببینیم، برای تولید یـک تراشـه ٤٥ نـانومتری کـه کارکردهای فرکانس بالا و آنالوگ را داشته باشد، چه تحولی باید در فناوری تولید و مواد جدید به وجود بیاید.

مزیت‌هایی که چنین تراشه‌ای می‌تواند ایجاد کند می‌تواند شامل اندازه کوچکتر تراشه و پتانسیل برای عملکرد بهتر و مصرف کمتر انرژی با همان کارکرد باشد که البته این بستگی دارد که محققان تا چه حد به موفقیت دست یابند .

WIFI &WIMAX-٦

١-٦مروری بر پیاده‌سازی شبکه‌هایWiMax

٢-٦یا وای مکس با وای فای رقابت خواهد کرد؟ --> Wi-Fi Will WiMAX compete with

٣-٦استاندارد جدید IEEE ٨٠٢ . ١١ n

مقدمه :

ایجاد امکان دسترسی به اینترنت پرسرعت به صورت بی‌سیم، سال‌هاست که مد نظر ارائه‌دهندگان سرویس در سراسر جهان می‌باشد. معمولاً در حوزه های تحت پوشش اپراتورها مناطقی وجود دارد که ارائه خدمات ارتباطی به‌صورت سنتی امکان پذیر نمی‌باشد و یا هزینه بالایی در بر دارد. این مناطق معمولاً در حومه شهرها قرار داشته و جمعیت کمی دارند.

اشاره :

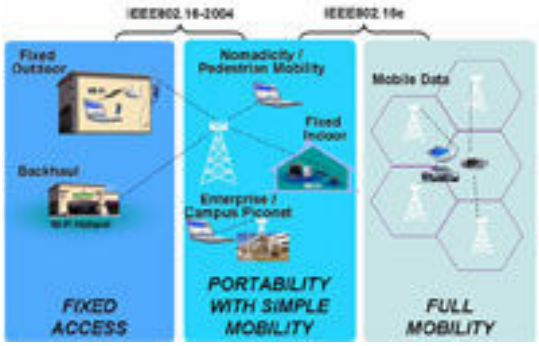
ایجاد زیرساخت‌های سیمی برای این نقاط مقرون‌به‌صرفه نمی‌باشد. استفاده از تکنولوژی WiMAX راه‌حل بهینه‌ای است که از جانب اپراتورها با استقبال زیادی روبه رو شده است. در شماره ۵۰ ماهنامه شبکه درباره استاندارد IEEE ۸۰۲,۱۶ که با نام تجاری WiMAX شناخته می‌شود و استاندارد شبکه‌های بی‌سیم شهری است، مطالب مفصلی ارائه گردیده است. در این شماره در نظر است با مروری کلی بر عملکرد این استاندارد، نحوه پیاده سازی شبکه های مبتنی بر آن بیان شود.

مروری بر پیاده‌سازی شبکه‌های WiMax

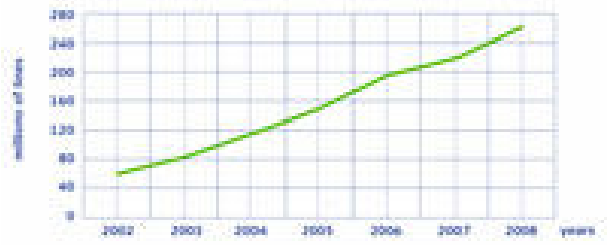
همان‌طور که در مقالات قبلی اشاره گردید، این استاندارد باندهای فرکانسی مختلفی را در محدوده‌های بامجوز و بدون‌مجوز متناسب با ساختار خود تحت پوشش قرار می‌دهد و استاندارد امکان ارائه خدمات بی‌سیم را به صورت ثابت و متحرک فراهم می نمایند.

شرح			استاندارد
Fixed / Mobile	Bit Rate	فرکانس	
Fixed (NLoS)	۳۲-۱۳٤ Mbps at ۲۸MHz	۲-۱۱ GHz	۸۰۲,۱٦a
Fixed (NLoS)	۳۲-۱۳٤ Mbps at ۱۲۸ MHz	٥ , ٦ GHz	۸۰۲,۱٦b
Fixed (LoS)	۳۲-۱۳٤ Mbps at ۱۲۸ MHz	٦٦ -۱۰ GHz	۸۰۲,۱٦c
Fixed (NLoS)	Up to ۷٥ Mbps at ۲۰ MHz	۲-۱۱ GHz	۸۰۲,۱٦d
Mobile (NLoS)	Up to ۱٥ Mbps at ٥ MHz	< ٦>	۸۰۲,۱٦e

۱ جدول



شکل ۱- دامنه کاربرد بخش‌های مختلف استانداردهای IEEE ۸۰۲,۱٦



نمودار ۱

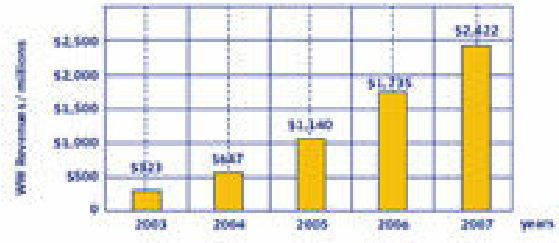
بخش‌هایی از این استاندارد در سال ۲۰۰٤ به رسمیت شناخته شد و در حال حاضر محصولات متعددی بـر پایـه آن ساخته و وارد بازار شده‌اند، اما بخش‌هایی مانند IEEE ۸۰۲,۱٦e که در شبکه‌های موبایـل کـاربرد دارد، هنـوز بـه عنوان یک استاندارد رسمی معرفی نشده است و درنتیجه هنوز هیچ تجهیزاتی مبتنی‌بر این استاندارد به تولیـد انبـوه نرسیده است. در جدول یک مقایسه‌ای بین استانداردهای مختلف و فرکانس کاری و نرخ بیتی آن‌ها دیده مـی‌شـود. مطالعات اخیر در زمینه میزان رشد تقاضا برای استفاده از این تکنولوژی نشان می‌دهد که تنها در چند سـال گذشـته تعـداد خطـوط نـصب‌شـده، از ۵۷ میلیـون در سـال ۲۰۰۲ بـه ۸۰ میلیـون در سـال ۲۰۰۳ افـزایش یافتـه اسـت. این میزان رشد، صعودی باورنکردنی دارد و پیش‌بینی می‌شود تعداد این خطوط تا سال ۲۰۰۸ مطابق نمودار ۱ رشد نماید.

روش‌های دسترسی مبتنی بر DSL) WDSL بی‌سیم) در مقایـسه بـا دسترسـی از طریـق خطـوط DSL از هزینـه کمتری برخوردارند، در نتیجه به سرعت در مکان‌هایی که امکان ارائه خـدمات ارتبـاطی وجـود نـدارد و یـا تـراکم جمعیت به اندازه‌ای است که ایجاد زیرساخت سیمی مقـرون بـه صـرفه نمـی‌باشـد جـایگزین روش‌هـای موجـود می‌شوند. بدنه رگولاتوری دولت‌ها نیز از این تکنولوژی به عنوان ابزاری برای از بین بـردن فاصـله دیجیتـالی بهـره می‌برند. به این منظور اقدام به بازنگری در فرکانس‌های موجود در باندهای با مجـوز و بـدون‌مجـوز نمـوده‌انـد تـا به‌واسطه آن بتوانند از طیف‌های فرکانسی مطرح در این تکنولوژی پشتیبانی نمایند. از نقطه‌نظر بازگشت سرمایه نیـز این فناوری قابل تامل است. همان‌طور که در نمودار ۲ مشاهده می‌شود، شروع ۲۳۲ میلیون دلاری و تخمـین رشـد

تا ۱/۷۵ میلیارد دلار در سال ۲۰۰۶ برای بازگشت سرمایه در این فناوری، یک رشد قابل‌ملاحظه اقتصادی است که مشوق اصلی اپراتورها در ایجاد شبکه‌های مبتنی‌بر این تکنولوژی محسوب می‌شود.
هر یک از تجهیزات مورداستفاده در این تکنولوژی شامل تجهیزات سمت مشترک، تجهیزات Station Base و تجهیزات لایه هسته و توزیع هر کدام به تنهایی در ایجاد هزینه‌های پیاده‌سازی سهیم می‌باشند. جدول ۲ نوع سرمایه گذاری برای هر یک از تجهیزات را نشان می دهد.

با استفاده از این تکنولوژی سرویس‌های متعددی را می‌توان در نواحی حاشیه‌ای شهرها و مناطق تجاری ارائه نمود.

هزینه های سرمایه گذاری تجهیزات	نوع سرمایه گذاری	نحوه تاثیر بر بازگشت سرمایه
تجهیزات لایه هسته و توزیع	سرمایه گذاری به صورت یکباره برای پوشش کلیه نقاط شبکه انجام می پذیرد	APEXکلی بین مشترکین تقسیم می گردد. مثلاً در مناطق پرجمعیت به ازای هر کاربر کمتر از ۱۰ دلار در نظر گرفته می‌شود.
تجهیزات Base Station	این سرمایه گذاری به صورت فازبه‌فاز متناسب با پیشرفت پروژه انجام می‌شود .	APEXدر این قسمت بین هر ۱۰۰۰ مشترک تقسیم می‌شود. به طور معمول CAPEX به ازای هر مشترک کمتر از ۱۰۰ دلار برای هر BS در ماکزیمم ظرفیت در نظر گرفته می‌شود .
تجهیزات CPE	این سرمایه گذاری نیز به‌صورت فازبه‌فاز انجام می‌شود. میزان سرمایه متناسب با نیازهای مشترکین متغیر می‌باشد .	بازگشت سرمایه در این قسمت متناسب با نحوه ارائه خدمات می‌باشد. به طور مثال بیشترین بازگشت سرمایه زمانی است که تجهیزات CPE به مشترکین اجاره داده می‌شوند و کمترین بازگشت سرمایه زمانی است که مشترکین تجهیزات سمت خود را خریداری می‌نمایند .
جدول۲		



نمودار۲

جدول ۳ سرویس‌های قابل‌ارائه در مناطق روستایی و حومه شهرها و درآمد ماهیانه برای پیاده‌سازی این سرویس‌ها با پهنای باند مشخص را نشان می‌دهد .

نوع سرویس	پهنای باند	ضریب Overbooking	متوسط درآمد ماهانه از مشترکین روستایی
دسترسی به اینترنت	۳٤۸ Kbps	٤۰:۱	۱۵
سرویس VoIP	۱۲۸Kbps	٤:۱	۵ $
جدول۳			

شکل ۳

سرویس‌هایی که با استفاده از این تکنولوژی در مناطق تجاری قابل‌پیاده‌سازی می‌باشد، عبارتند از: سرویس‌های عمومی که شامل دسترسی به اینترنت، سرویس‌های صوتی، تصویری و از این قبیل می‌باشد و سرویس‌های تجاری که عموماً با تجارت‌الکترونیکی مرتبط است و دارای ویژگی‌های خاص خود از لحاظ امنیتی و کیفیت می‌باشد. این سرویس‌ها با توجه به ماهیتشان، غالباً از پهنای باند بالایی استفاده می‌کنند. در نتیجه درآمد ناشی از ارائه آن‌ها نیز برای اپراتورها قابل‌ملاحظه می‌باشد.

پیاده سازی WiMAX

فناوری WiMAX دارای مزایای زیادی است که آن‌را بر سایر تکنولوژی‌های موجود در زمینه شبکه‌های بی‌سیم ارجح می‌سازد.

این مزایا عبارتند از:

- ❖ کیفیت سرویس
- ❖ کارآیی بالا
- ❖ ساختار استاندارد
- ❖ پشتیبانی از آنتن های هوشمند

تجهیزاتی که برای پیاده‌سازی شبکه‌های شهری مورداستفاده قرار می‌گیرند در سه لایه تجهیزات سمت مشترک (CPE) تجهیزات مربوط به Base Stationها و تجهیزات لایه هسته شبکه می‌باشد. تجهیزات مربوط به سمت مشترک به‌طور کلی به‌گونه‌ای پیکربندی می‌شوند تا بتوانند کلیه اطلاعات مربوطه را با فرکانس‌های رادیویی به نزدیکترین Base Station انتقال دهند .

مرحله بعدی در ایجاد شبکه شهری بی‌سیم ایستگاه‌های ارائه‌دهنده سرویس است که به POP یا CO معروفند، این ایستگاه‌ها باید به‌گونه‌ای طراحی شوند که امکان تخصیص پهنای باند حداقل ۱Mbps را برای هر مشترک تضمین نمایند. هرگونه ارتباطی با شبکه سایر ارائه‌دهندگان سرویس از طریق این نقاط صورت می‌پذیرد

ساختار این تکنولوژی به‌گونه‌ای است که می‌توان آن‌را در هر قسمت از شبکه مورداستفاده قرار داد، اما بهینه‌سازی نحوه استفاده از این تکنولوژی به هزینه آن نیز بستگی دارد. همان‌گونه که در بررسی‌های اقتصادی انجام‌شده دیده می‌شود، این فناوری در لایه دسترسی قابل‌جایگزینی برای سایر تکنولوژی‌های مطرح در زمینه بی‌سیم می‌باشد.

نـــوع سرویس	پهنای باند	ضـــــــــــریب Overbooking	متوسط درآمد ماهانه از مشترکین تجاری
سـرویس هـــای عمومی	۵۱۲Kbps	٤:۱	۷۵ $
سـرویس هـــای تجاری	۱Mbps	٤:۱	۱۰۰ $

جدول٤

با استفاده از این تکنولوژی می‌توان در لایه توزیع (Backhaul) و دسترسی (Last Mile) با صرف هزینه پـایین، کارآیی بالایی ایجاد نمود. از WiMAX برای مجتمع‌سازی WiFi نیـز اسـتفاده مـی‌شـود. درحـال حاضـر بـرای بهینه‌سازی شبکه‌های بی‌سیم، توصیه می شود با بهره‌گیری از قابلیت‌های هریک از تکنولوژی‌های مطـرح در زمینـه ایجاد شبکه‌های بی‌سیم از هر دو تکنولوژی WiMAX و WiFi در کنار یکدیگر اسـتفاده شـود. بـه ایـن ترتیـب می‌توان از قابلیت های هر یک به صورت بهینه بهره برد.

همان‌گونه که مشاهده می‌شود در شبکه‌های محلی و Campus از همبندی Mesh تکنولوژی WiFi استفاده شده است و برای لایه توزیع (Backhaul) نیز WiMAX مورداستفاده قرار گرفته است .

انجمن WiMAX این استاندارد را برای پیاده‌سازی ارتباطات نقطه به نقطـه (P۲P) و یـک نقطـه بـه چنـد نقطـه (P۲MP) در مناطق روستایی و حومه شهرها که از تراکم جمعیت بالایی برخوردار نمی‌باشند،

آیا وای مکس با وای فای رقابت خواهد کرد؟ <-- Wi-Fi Will WiMAX compete with

به روشنی واضح است که **وای مکس** و **وای فای** تکنولوژی های مکمل یکدیگرند و برای آینده ای قابل پیش بینی به همین صورت خواهند ماند. تکنولوژی **وای فای** که به طور گسترده ای در دسترس می باشد و در نواحی متمرکزی چون هتل ها، رستوران ها، فرودگاه ها و حتی در مناطق گسترده تری در بعضی از شهرها مورد استفاده قرار می گیرد، برای سال های زیادی به رشد خود ادامه خواهد داد.

مقبولیت گسترده و پروتکل جامع و یکپارچه b/g/a ۸۰۲,۱۱ در امواج رادیویی کامپیوتر های laptop، رشد دائمی بر پایه مصرف کنندگان **وای فای** فراهم می سازد. گروه Forum حداقل سه موج از ابزار **وای مکس** را در طول دو سال آینده پیش بینی می کند که برای کامپیوتر های laptop (سیار) مقرون به صرفه می باشد و بر پایه امواج رادیویی **وای مکس** بنا نهاده شده است که سومین موجی است که در سال های ۲۰۰٦ تا ۲۰۰۷ عرضه خواهد شد.

هر چند حتی این واحد ها تقریبا دوگانه می شوند (**وای فای** / **وای مکس**) ، یا اینکه چندگانه خواهد شد (**وای فای** / **وای مکس** / **سلولی**) و برای چندین سال بعد از آن به کارشان ادامه خواهند داد. همانطوری که استاندارد **وای مکس** رشد می کند و برای بدست آوردن پذیرش و کاهش هزینه های پیشرفت خود راه هایی می گشاید، تراشه های جدیدتری هستند که توانایی کارکرد در طول پایگاه های چند گانه را با هم ترکیب می کنند و با بخش شبکه های شهری مشترک می شوند که آنها نیز به آرامی تبدیل به سیستم های **وای مکس** قدرتمندی برای حالت های تجاری آن می شوند که از مزیت حوزه ها و نواحی متمرکز نیز بهره مند می شوند.

اساسا این بدان معناست که کاربران **وای مکس** در چند سال آینده قادر خواهند بود نه تنها به نواحی متمرکز **وای فای** مثلا در یک کافی نت دسترسی داشته باشند بلکه همچنین می توانند دسترسی سیار وای مکس را نیز در سراسر شهر به همان خوبی داشته باشند.

به هر حال سایر استاندارد های تکنولوژی LAN به عنوان مثال بلوتوث، Ultraband و خصوصیات دیدار شده در پروتکل n۸۰۲,۱۱ که مقدار کمتری را از لحاظ برد شبکه های نواحی متمرکز ارائه می دهند نیز تراشه ها و امواج رادیویی کامپیوترهای لپ تاپ خود را گسترش داده و ملزوم می سازد که در نهایت قادر باشند.

به طور دائمی و به خوبی از این بردهای کوتاهتر شبکه های داده **سلولی** و شبکه های **وای مکس** شهری بگذرند. استاندارد **وای مکس** بخش اصلی دیدگاه درخشان آینده ی بی سیم پهن باند می باشد که این انعطاف پذیری را وعده می دهد.

انواع مختلف اتصالها با یکدیگر در زیر مقایسه شده اند:

نوع	سرعت	محدوده (برد)	شرح
IrDA (مادون قرمز)	۹/٦ کیلو بیت تا ۱۱۵ کیلو بیت تا (٤ مگا بیت)	کمتر از ٦ فیت	۱- از طریق مادون قرمز تبادل اطلاعات می کنند، ۲- از قدرت وانرژی کمتری استفاده می کنند.
وای فای (Wi-Fi)	۱مگا بیت تا ٥٤ مگا بیت	جدول زیر را ملاحظه نمایید	وای فای (Wi-Fi) به هر سه نوع خدمات بی سیمی که مدل ۸۰۲,۱۱ که در جدول زیر نشان داده ایم ، اشاره میکند همینطور به دسته بندیهای جدیدی که در آینده ارائه خواهد شد ، این تکنولوزی همانند یک شبکه عادی از طریق سیم از جنبه های مختلف عمل میکند. این تکنولوژی یا در درون دستگاه نصب شده و یا به شکل کارتها یا رابطهای قابل اضافه شدن به کامپیوترهای رومیزی یا همان لپ تاپها در دسترس می باشد.
۸۰۲,۱۱a	۱ تا ٥٤ مگا بیت	٥۰ تا ۱٥۰ فیت فاصله	از این تکنولوژی زیاد بصورت همگانی استفاده نمی شود، همچنین این روش نسبت به مدل ۸۰۲,۱۱b/g از فرکانس متفاوتی استفاده می کند .
۸۰۲,۱۱b	۱ تا ۱۱ مگا بیت	۱۰۰ تا ۳۰۰ فیت فاصله	روشی است ، که در حال حاضر بیشترین استفاده را دارد.
۸۰۲,۱۱g	۱ تا ٥٤ مگا بیت	۱۲۰ تا ۳٥۰ فیت فاصله	آخرین روشی است که با مدل ۸۰۲,۱۱b سازگار میباشد.
بلوتوث	۱۲۰ کیلوتا ۷۲۳ کیلو بیت	۳۰ تا ۳۰۰ فیت	۱- از این سیستم برای وسایل و دستگاههایی که ازنسل کامپیوتر هستند، استفاده می شود. ۲- دارای برد ۳۰ فوتی میباشد. ۳- طریقه نصب آن اینست که یا در خود دستگاه نصب میشود ، و یا بصورت کارتهایی است که قابل اضافه شدن به دستگاه میباشند .

GPRS	کمتر از ۱۱۵ کیلو بیت	هر جایی که برای پوشش تلفن همراه مناسب باشد	۱- خدمات دیتایی است که توسط تلفنهای همراه ، که تحت شبکه GSM هستند استفاده میشود ۲- سرعت آن حدود ۳۰ کیلو بیت در ثانیه است ، این سرعت بستگی به تعداد کاربرهایی دارد ، که از این خدمات بصورت مشترک در زمان تعیین شده استفاده میکنند. ۳- همچنین اینها یک سرویس و خدماتی از نسل ۲/۵ تلفنهای همراه به حساب می آیند .
نسل ۲/۵	سرعت آن مختلف بوده و تا حدود ۱۲۸ کیلو بیت میباشد.	هر جایی که برای پوشش تلفن همراه مناسب باشد.	بنابر توافقهایی بعمل آمده این نسل هنوز آماده ارائه خدمات همیشه برقرار برای نسل سوم نمی باشد، تمامی شرکتهای تلفنهای همراه امیدوار هستند، که اگر تامین مالی شان و تکنولوژی اجازه دهد، آنرا معرفی کنند.
نسل سوم (۳G)	۲ مگا بیت در حال سکون، ۳۸٤ کیلو بیت در حال حرکت با سیگنال خوب . ۱٤٤ کیلو بیت در حرکت سریع دارای سیگنال ضعیف	هر کجا که برای تلفن همراه مناسب باشد	انتقال دیتا را بطور بسیار سریع برای کاربرانش فراهم می آورد، به مدل پی سی اس اسپیرینت (PCS Sprint) و ای تی اند تی اج (AT&T) (EDGE) (۱۰۰ تا ۱۳۰ کیلو بیت) که در حال حاضر در ایالات متحده موجود است ، نزدیک میباشد .
مودم	کمتر از ٥٦ کیلو بیت.	هرجایی که بصورت بی سیم نمی باشد.	روش قدیمی است که باید از طریق کامپیوتر برای وارد شدن به اینترنت از روش شماره گیری (Dial-Up) استفاده نماید .
DSL / کابل	۱۰۰ کیلو بیت تا ۱/۵ مگا بیت	بصورت بی سیم نمی باشد.	۱-بی سیم نمیباشد. ۲- با یک باند پهن، وسایل را به اینترنت متصل می کند .
شبکه محلی(LAN)	۱۰مگا بیت تا ۱۰۰ مگا بیت	بصورت بی سیم نمی باشد.	۱- بی سیم نمی باشد. ۲- متداولترین نوع شبکه ای است که با کابل کار میکند.

واژه نامه شبکه های بیسیم

G۲ : امروزه رایج‌ترین نوع ارتباط تلفنی بی‌سیم است که ارتباطات اطلاعاتی کندی را فراهم می‌سازد و تمرکز اصلی آن روی کیفیت صدا است.

G۲,۵ : یک استاندارد حد وسط و رابط بین G۲ و G۳ است. برقراری ارتباط به طریقه دیجیتال زمینه پست الکترونیکی و مرور وب آسان را فراهم می‌سازد.

G۳ : به عنوان سومین نسل از تکنولوژی ارتباطات بی‌سیم عمل می‌کند و حاکی از پیشرفت‌های سریع و قریب الوقوع در ارتباطات صوتی و اطلاع‌رسانی بی‌سیم با انواع استانداردهای موجود می‌باشد. مصرف اصلی این تکنولوژی، بالا بردن سرعت انتقال داده به ۲ مگابیت در ثانیه است.

۸۰۲,۱۱ : گروهی از ویژگی‌های بی‌سیم می‌باشد که از سوی IEEE عرضه می‌شود و شامل رابط بی‌سیمی بین دستگاه‌ها برای کنترل ترافیک بسته‌های اطلاعاتی است (برای اجتناب از برخورد در انتقال داده و غیره). این ویژگی‌ها با علائم و نشانه‌های متفاوتشان شامل موارد زیر هستند.

a۸۰۲,۱۱ : با دامنه فرکانس ۵ گیگاهرتز (۵,۱۲۵ تا ۵,۸۵ گیگاهرتز) و حداکثر سرعت سیگنال ٥٤ مگابیت در ثانیه عمل می‌کند. باند فرکانس ۵ گیگاهرتز به اندازه فرکانس ۲,٤ گیگاهرتز شلوغ نیست، چون کانال‌های بیشتری نسبت به b۸۰۲,۱۱ دارد و در واقع از b۸۰۲,۱۱ جدیدتر است، ولی با آن سازگاری ندارد.

b۸۰۲,۱۱ : در باند ۲,٤ گیگاهرتزی،Industrial, ۲,٤(ISM) Scientific and Measurement تا ۲,٤۸۳۵ گیگاهرتز عمل می‌کند و میزان سیگنال‌دهی آن تا ۱۱ مگابیت در ثانیه است که معمولا این میزان فرکانس کاربرد بیشتری دارد، مثل اجاق‌های مایکروویو، تلفن‌های بی‌سیم، تجهیزات علمی و پزشکی که همه همچون دستگاه‌های بلوتوث با باند ۲,٤ گیگاهرتز ISM کار می‌کنند.

e۸۰۲,۱۱ :این استاندارد در اواخر ماه سپتامبر سال ۲۰۰۵ توسط IEEE تصویب شد. کیفیت سرویس دهی آن طوری است که می‌تواند کیفیت ترافیک صوتی و تصویری را تضمین نماید و برای شرکت‌هایی حائز اهمیت است که به استفاده از تلفن‌های Wi-Fi تمایل دارند.

g۸۰۲,۱۱ : شبیه b۸۰۲,۱۱ است، ولی این استاندارد از میزان سیگنال‌دهی تا ٥٤ مگابیت در ثانیه پشتیبانی می‌کند، همچنین در باند ISM، ۲,٤ گیگاهرتز کاربرد دارد، ولی از تکنولوژی رادیویی متفاوتی برای افزایش ظرفیت پذیرش کلی استفاده می‌کند؛ با b۸۰۲,۱۱ قدیمی نیز سازگار است.

i۸۰۲,۱۱ : گاهی ۲ WPA (Wi-Fi Protected Access ۲) نامیده می‌شود و در ژوئن سال ۲۰۰٤ به تصویب رسیده است. ۲ WPA از Encryption Standard Advanced (استاندارد رمزگذاری پیشرفته) در حد ۱۲۸ بیت و بالاتر از آن پشتیبانی می‌کند و با ویژگی‌های کنترل کلید و شناسایی کاربر x۸۰۲,۱ همراه است.

k۸۰۲,۱۱ : در اواسط سال ۲۰۰٦ به تصویب می‌رسد و استاندارد Radio Resource Management (کنترل منابع رادیویی) است که اطلاعات سنجش نقاط دستیابی و تغییرات لازم برای اجرای بهتر LAN (شبکه‌های) بی‌سیم را فراهم می‌سازد. مثلا می‌تواند با استفاده از نقاط دستیابی، بار ترافیک را مدیریت نماید یا به تنظیم مرتب و دائم نیروی انتقال داده، جهت کاهش تداخل (داده‌ها) کمک نماید.

n۸۰۲,۱۱ : این استاندارد بهینه‌سازی برای توان عملیاتی بالاتر و برای بالا بردن ظرفیت پذیرش WLAN تا بیش از ۱۰۰ مگابیت در ثانیه طراحی شده است. این استاندارد در اواخر سال ۲۰۰٦ به تصویب نهایی می‌رسد.

r۸۰۲,۱۱ : این استاندارد در سال جاری به تصویب می‌رسد و یک استاندارد گشت و گذار سریع است که برای حفظ ارتباط‌پذیری کاربر در هنگام جابه‌جایی و حرکت از یک نقطه دستیابی به نقطه دیگر به کار می‌رود، همچنین در برنامه‌های کاربردی که به استانداردهای کیفیت خدمات بالا با تاخیر کم، مثل کیفیت صدای روی WLAN نیاز دارند، مهم است.

s۸۰۲,۱۱ : این استاندارد در شبکه‌بندی mesh به کار می‌رود و در اواسط سال ۲۰۰۸ به تصویب خواهد رسید.

Access Point(نقطه دستیابی) : یک فرستنده/گیرنده WLAN یا Base station است که می‌تواند یک شبکه را به شبکه دیگر یا چند دستگاه بی‌سیم وصل نماید. نقاط دستیابی (APها) به عنوان پل و رابطی برای یکدیگر هستند.

حالت Ad hoc : یک چهارچوب شبکه بی‌سیم است که در آن دستگاه‌ها بدون اینکه لازم باشد از یک AP استفاده کنند یا به شبکه وصل شوند، قابلیت برقراری ارتباط مستقیم با یکدیگر را خواهند داشت و درست برعکس شبکه زیربنایی است که در آن همه دستگاه‌ها از طریق AP به یکدیگر وصل شده و ارتباط برقرار می‌نمایند.

بلوتوث : یک لینک (اتصال) رادیویی کم هزینه با بورد کوتاه بین لپ‌تاپ‌ها، تلفن‌های همراه، نقاط دستیابی شبکه و دستگاه‌های دیگر است. بلوتوث می‌تواند جایگزین کابل‌ها شود و برای ایجاد شبکه‌های ad hoc مفید باشد، همچنین روش استانداردی را برای اتصال دستگاه‌ها در هر جای دنیا ارائه می‌دهد.

Code Division Multiple Access : یا CDMA یک تکنولوژی سلولی دیجیتال است که از تکنیک‌های طیف گسترده استفاده می‌کند و به جای جداسازی کاربران از یکدیگر آنها را با استفاده از کدهای فرکانس دیجیتال با دسترسی کامل به طیف، جدا می‌سازد. CDMA با GSM و TDMA رقابت می‌کند.

CDPD : تکنولوژی Cellular Digital Packet Data برای حاملان ارتباطات از راه دور کاربرد دارد که آن را برای انتقال داده به کاربران از طریق شبکه‌های سلولی آنالوگ استفاده نشده به کار می‌برند. اگر یک قسمت از شبکه مثل یک محدوده جغرافیایی خاص یا یک "سلول"، بیش از اندازه استفاده شود، CDPD می‌تواند بطور خودکار منابع شبکه را برای کنترل ترافیک اضافه به کار برد.

Internet Association & Cellular Telecommunications : یا CTIA یک سازمان بین‌المللی است که به معرفی و عرضه همه عناصر مخصوص ارتباطات بی‌سیم، مثل سرویس‌های ارتباطات شخصی، سلولی، سرویس‌های پیشرفته مخصوص ماهواره و رادیوی سیار، کمک کرده و توجه سرویس دهندگان، سازندگان و غیره را به خود جلب می‌کند.

EDGE : نرخ (سرعت) انتقال داده پیشرفته برای GSM Evolution است. این تکنولوژی G۳، انتقال داده به طریقه بی‌سیم را با سرعت ۳۸٤ کیلوبیت در ثانیه میسر می‌سازد و مبتنی‌بر تکنولوژی GSM بوده و امکان خدمات باندپهن بالایی، مثل مولتی مدیا (چند رسانه‌ای) را فراهم می‌سازد. در آمریکای شمالی از آن بیشتر پشتیبانی می‌شود، چون تکنولوژی‌هایی مثل CDMA و UMTS مورد توجه بوده و کاربرد بیشتری دارد.

Evolution Data Only یا Data Optimized Evolution : تکاملی از شبکه‌های CDMA است که بر مبنای استاندارد xRTT۱ کار می‌کند و سرعت انتقال داده بی‌سیم بیشتری را یعنی از ٤۰۰ کیلوبیت در ثانیه به ۷۰۰ کیلوبیت در ثانیه، با رکورد تقریبی ۲,٤ مگابیت در ثانیه فراهم می‌سازد.

FLASH-OFDM : یک تکنولوژی باندپهن سلولی اختصاصی است که اپراتورهای شبکه می‌توانند از آن برای کامپیوترهای نوت‌بوک کاربران در حال حرکت یا به عنوان یک سیستم دستیابی بی‌سیم ثابت استفاده کنند که برای

اتصال کامپیوترهای خانگی و اداری کوچک تا آخرین مسافت، جواب می‌دهد. ویژگی‌های مهم آن، معماری IP کامل و سرعت بالای آن است. این تکنولوژی به کاربران امکان می‌دهد تا با سفر در حد ۲۵۰ کیلومتر در ساعت، داده را با سرعت ۱,۵ مگابایت در ثانیه دریافت کنند یا با سرعت ۵۰۰ کیلوبیت در ثانیه آن را ارسال نمایند.

Division Multiplexing Orthogonal Frequency یا (OFDM) با تبدیل سیگنال‌های رادیویی به سیگنال‌های کوچکتر و با سرعت پایین‌تر که به صورت موازی منتقل می‌شوند، اختلال ایجاد شده هنگام انتقال را کاهش داده و از باندپهن کافی استفاده می‌کند، ولی بورد آن را کاهش می‌دهد.

GPS یا Global Positioning System : "منظومه‌ای" از ٢٤ ماهواره است که زمین را در ارتفاع ۲۰،۲۰۰ کیلومتری دور می‌زند و استفاده از گیرنده‌های زمینی را برای افراد، جهت شناسایی موقعیت جغرافیایی آنها بین ۱۰ تا ۱۰۰ متر امکان‌پذیر می‌سازد. این ماهواره‌ها از محاسبات ریاضی ساده‌ای برای پخش اطلاعات استفاده می‌کنند که به عنوان طول و عرض و ارتفاع جغرافیایی، توسط گیرنده‌های زمین ترجمه شده‌اند.

GPRS : تکنولوژیGeneral Packet Radio Service با سرعت حداکثر ۱۱۵ کیلوبیت در ثانیه، در مقایسه با سرعت ٦/٩ کیلوبیت در ثانیه در سیستم‌های GSM قدیمی‌تر کار می‌کند؛ اینترنت و ارتباطات بی‌سیم دیگر با سرعت بالا، مثل پست الکترونیکی، بازی‌ها و برنامه‌های کاربردی را فعال و امکان‌پذیر می‌سازد، همچنین از حد وسیعی از باندپهن پشتیبانی کرده و در باندپهن محدود نیز کاربرد مناسبی دارد. برای ارسال و دریافت مقادیر کوچک داده، مثل نامه‌های الکترونیکی و مرور وب به همان اندازه مقادیر زیاد داده، مناسب است.

Communications Global System for Mobile : یا GSM (سیستم جهانی مخصوص ارتباطات تلفنی) یک سیستم سلولی دیجیتال مبتنی‌بر تکنولوژی باند باریک TDMAاست که به کاربران امکان دسترسی به اسلات‌های زمانی روی باندهای با همان فرکانس را می‌دهد، همچنین تا ۸ ارتباط همزمان با همان فرکانس را برقرار می‌سازد؛ این تکنولوژی رقیب DMAاست.

HSDPA یا High-Speed Downlink Packet Access : یک تکنولوژی داده با سرعت بالای G۳ است و در واقع همان استانداردWCDMA پیشرفته است که سرعت را بالا برده و میزان تاخیر را کاهش می‌دهد؛ با طیف ۵ مگاهرتز کار می‌کند و سرعت واقعی از ٤٠٠ کیلوبیت در ثانیه را به ٦٠٠ کیلوبیت در ثانیه می‌رساند؛ حداکثر سرعت تقریبی آن ٤/١٤ مگابیت در ثانیه می‌باشد.

Hot spot : مکانی مثل، هتل، رستوران یا فرودگاه که دسترسی Wi-Fi را به صورت رایگان یا با پرداخت هزینه امکان‌پذیر می‌سازد.

I-Mode : یک سرویس اینترنت بی‌سیم عمومی است که در سال ۱۹۹۹ به وسیله شرکت NTT DoCoMoدر ژاپن دایر گردید و برمبنای شکل ساده شده‌ای از HTML کار می‌کند و اطلاعات بسته‌ای، مثل بازی‌ها، نامه‌های الکترونیکی و حتی برنامه‌های بازرگانی را برای دستگاه‌های کوچک دستی ارسال می‌کند.

IEEE یا Institute of Electrical and Electronics Engineers : یک سازمان غیرانتفاعی فنی حرفه‌ای با بیش از ۳۶۰۰۰۰ کارمند اختصاصی در بیش از ۱۷۵ کشور است که در زمینه‌های فنی، مثل مهندسی کامپیوتر و ارتباطات از راه دور تخصص و صلاحیت دارد؛ این سازمان ویژگی‌های ۸۰۲,۱۱ را نیز توسعه داده است.

MAC : هر دستگاه بی‌سیم۸۰۲,۱۱ دارای یک آدرسMedia Access Controlمنحصر به خود است که درون آن بصورت کد و برنامه‌ای برای کنترل عملیات آن قرار گرفته است. این شناسه ویژه برای برقراری امنیت شبکه‌های بی‌سیم به کار می‌رود. وقتی یک شبکه از یک جدول MAC استفاده می‌کند، تنها رادیوهای ۸۰۲,۱۱ که دارای آدرس‌های MAC اضافه شده به جدولMAC شبکه بوده‌اند، می‌توانند به این شبکه دسترسی داشته باشند.

networking Mesh(شبکه‌بندی مش) : نمایانگر گره‌های شبکه بی‌سیم و مجزا است که با یکدیگر در ارتباط بوده و شبکه‌هایی را می‌سازند که خود را پیکربندی نموده و تنها با گره‌ای این کار را انجام می‌دهند که برای قرار گرفتن درون یک LAN (شبکه) دارای سیم لازم است.

MIMO یا Multiple Input Multiple Output : به استفاده از چند آنتن در یک دستگاه Wi-Fi به ارتقاء عملکرد و ظرفیت پذیرش اشاره می‌کند. تکنولوژی MIMO از یک ویژگی به نام multipath (چند مسیری) بهره می‌گیرد و زمانی اتفاق می‌افتد که یک مخابره رادیویی در نقطهAآغاز شده و سپس قبل از دریافت از چند سطح یا شیء و از چند مسیر در نقطه Bعبور می‌کند. تکنولوژیMIMO از چند آنتن برای جمع‌آوری و سازماندهی سیگنال‌هایی استفاده می‌کند که از طریق این مسیرها دریافت می‌شوند؛ این تکنولوژی بیشتر در استاندارد n۸۰۲,۱۱ کاربرد دارد.

RFID : شناسایی فرکانس رادیویی از فرستنده‌های رادیویی دارای برق ضعیف، برای خواندن اطلاعات ذخیره شده در یک tag فرستنده و گیرنده خودکار در فواصل بین ۲,۵ سانت تا ۳ متر استفاده می‌کند. TagهایRFID برای

کنترل دارایی‌ها، صورت موجودی و تایید و توصیه پرداخت‌ها به کار می‌روند و بیشتر به عنوان کلیدهای الکترونیکی در ابزارهای خودکار و تهدیدات امنیتی دیگر استفاده می‌شوند.

Roaming : عبارت است از جابجایی یک دستگاه سیار از یک مکان و وضعیت شبکه بی‌سیم به دیگری بدون هیچ وقفه یا اختلال در سرویس یا قطع اتصال.

Smart phone(تلفن هوشمند) : یک تلفن بی‌سیم با قابلیت‌های اینترنت و متن است که می‌تواند تماس‌های تلفنی بی‌سیم را کنترل نموده، آدرس‌ها را حفظ کند، پست صوتی را دریافت کرده، به اطلاعات روی اینترنت دست یافته و نامه‌های الکترونیکی و مخابره‌های فاکس را ارسال و دریافت نماید.

Site Survey (بررسی سایت) : در وضعیت یکWLANجدید برای اجتناب از اتلاف وقت و بروز مشکلات پرهزینه انجام می‌شود که شامل طراحی شبکه، کنترل روی ساخت و تجهیزات و آزمایش آنها است.

SMS یا Short Message Service (سرویس پیام کوتاه) : امکان ارسال پیام‌های متنی کوتاه بین دستگاه‌های سیار، مثل موبایل، دستگاه‌های فکس وBerry Black را فراهم می‌سازد. این پیام‌ها با تعداد ۱۶۰ حرف الفبایی، فاقد تصویر یا گرافیک به عنوان متنی روی صفحه نمایش دستگاه گیرنده ظاهر می‌شوند و با شبکه‌های GSM نیز کار می‌کنند.

SSI یا Service Set Identifier : یک سلسله کاراکتر منحصر به شبکه خاص یا بخشی از شبکه است که از شبکه و همه دستگاه‌های ضمیمه آن، برای شناسایی خود استفاده می‌کند و هنگامیکه بیش از یک شبکه مستقل در محلی نزدیک به هم وجود داشته باشند، به دستگاه‌ها امکان می‌دهند تا به شبکه درست متصل شوند.

Symbian Ltd : یک سرمایه‌گذاری مشترک بین شرکت‌هایLM Ericsson Telephone، موتورولا، نوکیا وPsion PLC برای توسعه سیستم‌عامل‌های جدید مبتنی‌بر پلات‌فرمEPOC۳۲شرکتPsionکه برای دستگاه‌های کوچک سیار و بی‌سیم، مثل تلفن‌ها و دستگاه‌های دستی مناسب می‌باشد.

TDMA یا Time Division Multiple Access : یک فرکانس رادیویی در دسترس را به یک شبکه درون اسلات‌های زمانی تقسیم می‌کند و سپس این اسلات‌ها را به چند تماس اختصاص می‌دهد، بنابراین یک فرکانس از چند کانال داده همزمان پشتیبانی می‌کند و می‌تواند نسبت به تکنولوژی‌های قدیمی‌تر از باندپهن استفاده بهتری

داشته باشد.TDMA در فرکانس‌های ۸۰۰ تا ۱۹۰۰ مگاهرتز در دسترس بوده و در سیستم سلولی دیجیتال GSMنیز به کار می‌رود.

UMTS یا Universal Mobile Telecommunications System : یک تکنولوژی شبکه سلولی G۳ است که از(Wideband Code WCDMA Division Multiple Access) استفاده می‌کند و از اواسط سال ۲۰۰۵ در ۲۵ کشور به اجر درآمده است. سرعت انتقال داده از ۳۸٤ کیلوبیت در ثانیه برای تلفن‌ها تا ۲ مگابیت در ثانیه برای دستگاه‌های ثابت می‌باشد.

UWB یا Ultrawideband : که پالس دیجیتال نیز نامیده می‌شود، یک تکنولوژی بی‌سیم مخصوص انتقال اطلاعات دیجیتال به بخش وسیعی از طیف فرکانس رادیویی با قدرت بسیار پایین است و چون به برق ضعیفی نیاز دارد، می‌تواند سیگنال‌ها را از بین درها و دیگر موانعی که معمولا سیگنال‌ها را در باندهای پهن محدودتر با نیروی قویتر منعکس می‌کنند، عبور دهد، همچنین می‌تواند مقادیر زیادی از داده را حمل نماید و برای سیستم‌های مکانهای رادیویی و راداری که به زمین احاطه دارند، مناسب است.

VoIP یا Internet Protocol Voice over : سیستمی برای ارائه ارتباطات صوتی رقمی شده (دیجیتالی شده) از طریق شبکه‌های IP است. این تکنولوژی به تلفن‌های دستی سازگار با یکدیگر یا کامپیوترهای دارای نرم‌افزار مناسب امکان می‌دهد تا تماس تلفنی برقرار نمایند.

WAP یا The Wireless Application Protocol : مجموعه‌ای از ویژگی‌ها است که به وسیله WAP Forum توسعه یافته است و به توسعه‌دهندگان امکان می‌دهد تا با استفاده از Wireless، برنامه‌های کاربردی شبکه‌بندی شده مناسب برای دستگاه‌های بی‌سیم دستی را بسازند.WAP برای کار با این دستگاه‌ها و محدودیت‌هایشان طراحی شده است: یک حافظه و اندازه cpu محدود، صفحه نمایش‌های کوچک و سیاه‌وسفید، باندپهن کم و اتصالات نامنظم.WAPیک استاندارد واقعی است که بیش از ۲۰۰ فروشنده از آن پشتیبانی می‌کند.

WCDMA یا Wideband Code Division Multiple Access : یک تکنولوژی بی‌سیم G۳ است که از CDMA نشات می‌گیرد و اطلاعات دیجیتالی شده را روی دامنه وسیعی از فرکانس‌ها، جهت افزایش سرعت ارسال می‌کند و از کانال‌های وسیع ۵ مگاهرتزی استفاده می‌نماید و برای بالا بردن سرعت با جایگزین کردن تکنولوژی

TDMA به جای CDMA به GSM و UMTS وابسته است. برای سرویس‌های تصویری، صوتی و اطلاع رسانی مفید بوده و می‌تواند با سرعت تا ۲ مگابیت در ثانیه داده را ارسال نماید.

WEP یا Wired-Equivalent Privacy protocol : در استاندارد۸۰۲,۱۱ IEEE برای ایجاد یک WLAN با حداقل سطح ایمنی و حفاظت، در مقایسه با یک LAN دارای سیم، با استفاده از رمزنگاری داده تعیین شده است. اکنون به خاطر طول نامناسب کلید و مشکلات دیگر آن ناقص شناخته شده و با وجود ابزارهای در دسترس می‌تواند به زودی مورد تهاجم قرار گیرد.

WME یا Wireless Multimedia Extensions : مجموعه‌ای از ویژگی‌های مبتنی بر استاندارد مقدماتی ۸۰۲,۱۱e IEEE است که ویژگی‌های اولیه QoS (کیفیت خدمات) را در شبکه‌های ۸۰۲,۱۱ IEEE ارائه می‌دهد. WME ترافیک برنامه‌های کاربردی مختلف، مثل برنامه‌های صوتی و تصویری را در محیط‌ها و شرایط مختلف در اولویت قرار داده است.

WPA یا Wi-Fi Protected Access : یک ویژگی رمزنگاری داده برای شبکه‌های بی‌سیم ۸۰۲,۱۱ است که جایگزینWEPضعیف‌تر شده است. WPA به وسیله اتحادیه Wi-Fi، قبل از تصویب استاندارد امنیتی۸۰۲,۱۱i توسط IEEE ایجاد شده و با استفاده از کلیدهای فعال وExtensible Authentication Protocol(پروتکل شناسایی کاربر قابل توسعه)، برای ایمن‌سازی دسترسی به شبکه و روشی برای کدگذاری به نام(TKIP) Temporal Key Integrity Protocol برای ایمن‌سازی ارسال اطلاعات،WFPرا بهینه می‌سازد.

WPA۲ یا ۲ Wi-Fi Protected Access : یک نسخه ارتقاء یافته از WPA است. WPA استاندارد رسمی ۸۰۲,۱۱i بوده که به وسیله IEEE در ژوئن ۲۰۰٤ به تصویب رسیده و به جای TKIP(فوق‌الذکر) از استاندارد Advanced Encryption استفاده می‌کند. AESاز کلیدهای ۱۲۸، ۱۹۲ و ۲٥٦ بیت پشتیبانی می‌نماید.

Wi-Fi یا Wireless fidelity : یک اصطلاح عمومی برای تکنولوژی۸۰۲,۱۱ است.

WLAN : شبکه‌های محلی بی‌سیم، از امواج رادیویی به جای کابل برای اتصال یک دستگاه کاربر استفاده می‌کنند، مثل اتصال لپ‌تاپ به یک LAN. آنها اتصالات اترنت را برقرار ساخته و در گروه و خانواده۸۰۲,۱۱ که ویژگی‌های آن به وسیله IEEE توسعه یافته است، به کار می‌روند.

War driving : به رانندگی با یک لپ‌تاپ با قابلیت بی‌سیم و آنتن برای یافتن مکانهایی جهت دستیابی به شبکه‌های بی‌سیم بی‌حفاظ، اشاره می‌کند. آنها معمولا شبکه‌های شرکتی بوده که در خارج از زیربنای واقعی شرکت توسعه یافته و به صورت بی‌حفاظ باقی مانده‌اند.

War chalking : علامت گذاری ساختمان‌ها یا پیاده‌روها با گچ برای نشان دادن محلی که می‌توان در آن به یک شبکه بی‌سیم شرکتی بدون حفاظ دسترسی پیدا کرد، این نقاط دستیابی از طریق همان war driving یافت شده‌اند.

WiMax : نام عمومی استاندارد شبکه بی‌سیم ۸۰۲,۱۶ مخصوص منطقه پایتخت است که باید تاکنون توسعه یافته باشد.WiMax که دارای برد ۵۰ کیلومتر می‌باشد و دستیابی به باند پهن شبکه با مشکل کمتر در دسترس‌پذیری و بدون پرداخت هزینه بابت به رشته درآوردن سیم‌ها (مثل دسترسی کامل در باندپهن) یا محدودیت‌های فاصله،Subscriber Digitalرا هدف قرار داده است. دو نوع WiMax وجود دارد: یکی ۸۰۲,۱۶-۲۰۰٤ یا d۸۰۲,۱۶ برای پیاده‌سازی‌های ثابت و e۸۰۲,۱۶ برای سرویس‌های متحرک.

WML یا Wireless Markup Language : مثل زبان برنامه‌نویسی اینترنتHTML است که محتوای اینترنت را به دستگاه‌های کوچک بی‌سیم، مثل تلفن‌های موبایل مجهز به مرورگر و دستگاه‌های دستی که دارای صفحه نمایش‌های کوچک و سی‌پی‌یوهای کند، ظرفیت حافظه محدود و باندپهن کم با قابلیت‌های ورودی محدود کاربر هستند، ارسال می‌کند.

Wi-Fi Alliance : یک سازمان بین‌المللی غیرانتفاعی که در سال ۱۹۹۹ برای تصویب قابلیت عمل محصولاتWLANمبتنی‌بر ویژگی۸۰۲,۱۱ IEEEدر چند محیط تشکیل شد. در حال حاضر نیز اتحادیه Wi-Fi دارای بیش از ۲۰۰ شرکت عضو از سراسر دنیا می‌باشد و بیش از ۱۰۰۰ محصول گواهینامه Wi-Fi را دریافت کرده است، یعنی از زمان شروع ارائه گواهینامه آن در مارس۲۰۰۰. هدف اعضای این اتحادیه، بالا بردن میزان آگاهی و تجربه کاربر .