

به نام خداوند جان و خرد
کزین برتر اندیشه برگزید

کتاب الکترونیکی

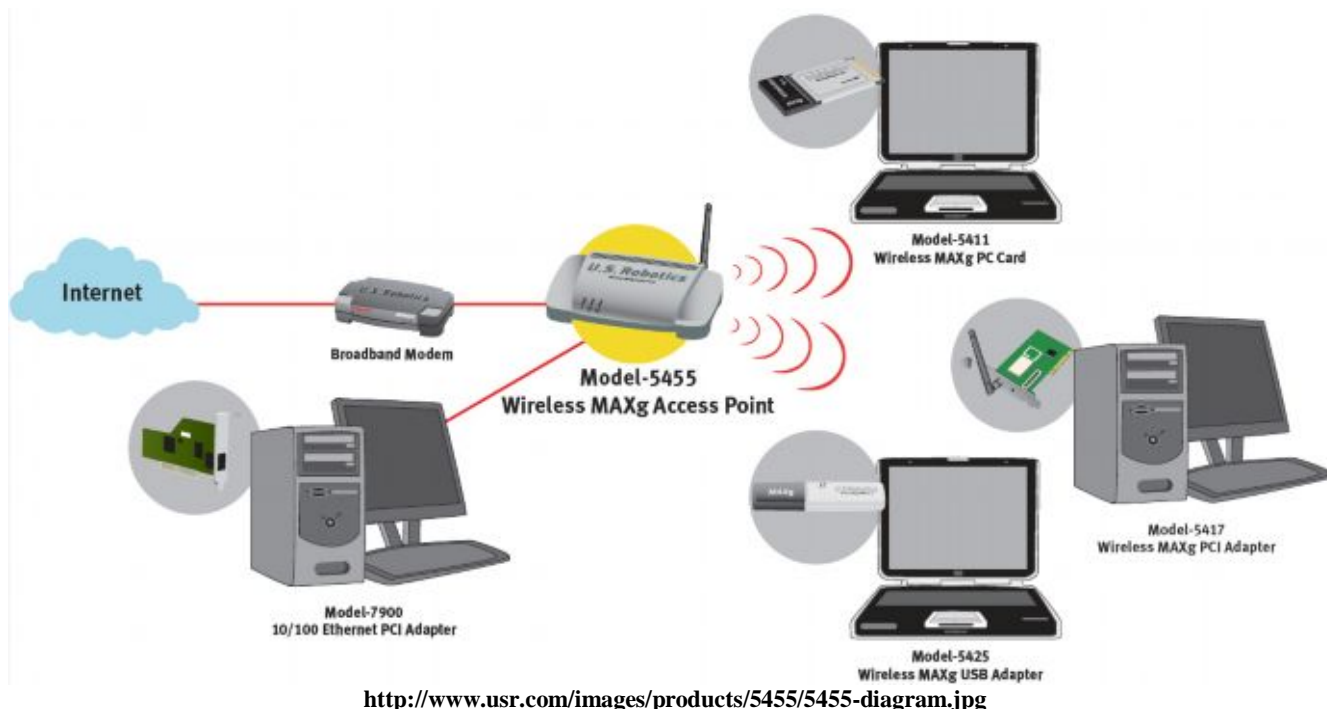
شبکه های بی سیم

Wireless Networks

By:

Morteza Hakimi Kia

Hardware Technician and Software Engineer



نوشته:

مرتضی حکیمی کیا- تکنسین کامپیوتر- مهندس نرم افزار

Email: Morteza_Hakimi@yahoo.com

پاییز و زمستان 1389

فهرست مطالب

صفحه	عنوان
1	پیشگفتار.....
	فصل اول - چرا شبکه بی سیم؟
4	1-1 شبکه های بی سیم چیستند؟.....
4	1-1-1 LAN ها ، WAN نیستند.....
6	2-1- فواید استفاده از شبکه های بی سیم.....
7	3-1- سرعت واقعی شبکه های بی سیم.....
8	1-3-1- سازگاری و هماهنگی شرکتهای سازنده.....
9	4-1- اشتراک گذاری مودم های پهن باند.....
10	1-4-1- پهن باند ایجاد شده توسط ماهواره.....
11	5-1- اشتراک گذاری چاپگرها و CD و هارددیسک ها.....
13	6-1- خلاصه فصل.....

فصل دوم - آماده سازی

16	1-2- آشنایی با بعضی از اصطلاحات شبکه سازی.....
18	2-2- شبکه های بی سیم چگونه کار می کنند؟.....
19	1-2-2- سایر شبکه های بی سیم.....
20	3-2- اشتراک سازی فایل ها.....
20	4-2- اشتراک سازی اینترنت.....
21	5-2- امنیت شبکه.....
21	1-5-2- رمز گذاری شبکه بی سیم.....
22	2-5-2- فیلترها (Filters).....
22	1-2-5-2- (Mac آدرس).....
22	2-2-5-2- دیوارهای آتش یا Firewalls.....
22	3-5-2- نرم افزارهای ویروس کش (Antivirus Software).....
23	6-2- خلاصه فصل.....

فصل سوم - ملاحظات بی سیم ها

- 3-1- مرتب سازی تجهیزات شبکه بی سیم 27
- 3-2- مد Ad-Hoc و Infrastructure (زیر ساخت)..... 27
- 3-3- چگونگی اثر گذاری اجسام روی سیگنال های بی سیم..... 30
- 3-4- ماکزیمم سرعت و سرعت های واقعی..... 30
- 3-5- نحوه دریافت سیگنال کامل از Wireless ها..... 30
- 3-6- استانداردهای 802.11 b و 802.11 a یا 802.11 g..... 31
- 3-7- خلاصه فصل..... 33

فصل چهارم - نصب سخت افزار و نرم افزار شبکه

- 4-1- گزینه های اتصال..... 36
- 4-1-1- کارتهای USB..... 37
- 4-1-2- کارت PCI..... 38
- 4-2- نصب سخت افزار..... 38
- 4-3- مرور نرم افزار..... 38
- 4-4- استفاده از مد Ad-Hoc..... 41
- 4-5- کار با Access Point ها..... 41
- 4-5-1 Access Point های دارای Router داخلی..... 42
- 4-6- رفع عیب یا Trouble shooting..... 43
- 4-7- نحوه قرار گرفتن تجهیزات..... 44
- 4-8- ایجاد شبکه peer-to-peer..... 44
- 4-9- نحوه ساخت یک شبکه ابتدایی..... 44
- 4-9-1- تنظیمات یک شبکه پیوندی..... 45
- 4-10- استفاده از دستگاههای چند رسانه ای شبکه..... 45
- 4-11- ترکیب نمودن تجهیزات 802.11..... 46
- 4-12- خلاصه فصل..... 47

فصل پنجم - ایجاد شبکه با استفاده از استانداردهای بی سیم

- 5-1- یک شروع خوب برای 802.11 b..... 50

- 50.....2-5- شبکه سازی بی سیم بصورت PDA
- 51.....3-5- Home RF
- 52.....4-5- حرکت به سوی 802.11 a
- 53.....5-5- پدیده ای نو بنام 802.11 g
- 53.....6-5- ارسال فایل ها از طریق اشعه مادون قرمز
- 55.....7-5- چاپ از طریق اشعه مادون قرمز
- 56.....8-5- خلاصه فصل

فصل ششم - آموزش گام به گام شبکه سازی در ویندوز 98

- 59.....1-6- اطمینان از شناسائی سخت افزار
- 61.....2-6- تست کردن برای TCP/IP
- 63.....3-6- نامگذاری کامپیوتر و گروه کاری
- 64.....4-6- شروع اشتراک گذاری فایل ها و چاپگر
- 66.....5-6- استفاده از شبکه مجاور یا Network Neighborhood
- 67.....4-6- دسترسی اشتراکی به اینترنت بصورت بی سیم
- 68.....4-6- خلاصه فصل

فصل هفتم - آموزش گام به گام شبکه سازی در ویندوز XP

- 71.....1-7- اطمینان از شناسائی سخت افزارها
- 73.....2-7- نصب و بروزرسانی درایوها
- 74.....3-7- تغییر تنظیمات دستی
- 75.....4-7- اشتراک سازی فایل و چاپگر
- 76.....5-7- اشتراک سازی دسترسی به اینترنت
- 77.....6-7- استفاده از جادوگر نصب شبکه یا Network Setup Wizard
- 81.....7-7- خلاصه فصل

فصل هشتم - روترها و اشتراک سازی اینترنت

- 84.....1-8- انتخاب کردن یک روتر بی سیم
- 85.....2-8- اضافه نمودن Router به شبکه
- 86.....3-8- نصب windows ICS روی کامپیوتر میزبان
- 86.....1-3-8- مراحل نصب ICS

- 8-4- تنظیم کامپیوترهای موجود در ایستگاه های کاری.....90
 8-5- خلاصه فصل.....91

فصل نهم - آماده سازی اینترنت

- 9-1- تنظیمات E-mail.....94
 9-2- مرور صفحات web.....97
 9-3- اضافه کردن امکانات پیام های فوری.....98
 9-4- پیدا کردن آدرس IP.....99
 9-4-1- در ویندوز 98 یا ME.....99
 9-4-2- در ویندوز 2000.....100
 9-5- تست توان عملیاتی یا Throughput.....101
 9-6- تنظیم کردن E یا PPP.....102

فصل دهم - رفع عیب اتصالات بی سیم

- 10-1- آیا درایورهای شبکه از نوع متداول و بروز هستند؟.....105
 10-2- تشخیص کارتهای شبکه معیوب105
 10-3- اشکالات شبکه ترکیبی ویندوز 98 و ویندوز 2000.....106
 10-4- پیکربندی سودمند خطاها.....107
 10-5- توقف یا hangup فایروال.....108
 10-6- اشکالات چاپگر.....111
 10-7- سایر اشکالات رایج.....112
 10-8- خلاصه فصل.....113

فصل یازدهم - امنیت

- 11-1- منشاء ضعف امنیتی در شبکه های بی سیم.....116
 11-1-1- برد و سطح پوشش.....116
 11-2- خدمات توزیع.....118
 11-3- مجتمع سازی.....119
 11-2- امنیت و پروتکل WEP.....119
 11-3- قابلیتها و ابعاد امنیتی استاندارد 802,11.....120

121.....	AUTHENTICATION -4-11
121.....	1-4-11-خدمات ایستگاهی
122.....	Confidentiality -2-4-11
122.....	Integrity -3-4-11
123.....	Authentication بدون رمزنگاری -5-11
123.....	Authentication با رمزنگاری RC4 -6-11
124.....	1-6-11- سرویس Privacy یا confidentiality
126.....	Integrity -2-6-11
126.....	3-6-11- ضعف های اولیه ای امنیتی WEP
127.....	4-6-11- استفاده از کلیدهای ثابت WEP
127.....	Initialization Vector - IV -5-6-11
127.....	7-11- ضعف در الگوریتم
128.....	1-7-11- استفاده از CRC رمز نشده
129.....	2-7-11- ویژگی های سیگنال های طیف گسترده
130.....	3-7-11- سیگنال های طیف گسترده با جهش فرکانسی
130.....	4-7-11- سیگنال های طیف گسترده با توالی مستقیم
131.....	استفاده مجدد از فرکانس
131.....	8-11- مقایسه استانداردهای 802.11
131.....	1-8-11- استاندارد 802.11 b
132.....	1-1-8-11- اثرات فاصله
133.....	2-1-8-11- پل بین شبکه ای
133.....	3-1-8-11- پدیده چند مسیری
133.....	2-8-11- استاندارد 802.11 a
135.....	1-2-8-11- افزایش پهنای باند
136.....	2-2-8-11- طیف فرکانسی تمیزتر
136.....	3-2-8-11- کانال های غیر پوشا
136.....	4-2-8-11- همکاری Wi-Fi
137.....	3-8-11- استاندارد بعدی IEEE 802.11g
142.....	منابع و مراجع

پیشگفتار

امروزه با پیشرفت تکنولوژی اطلاعات نیاز به استفاده از امکانات روز جهت تبادل داده ها با سرعت و دقت بالا و رهایی از محدودیت های محیطی بیشتر احساس می شود بنابراین لازم است از امکانات و تجهیزاتی استفاده شود که بتوان به سادگی و آسانی راه اندازی شده و استفاده نمود.

یکی از این روشها که راحت ترین و ساده ترین و کم هزینه ترین روش می باشد استفاده از شبکه های کامپیوتری بخصوص شبکه های کامپیوتری بی سیم است متأسفانه در کشور ما چندان به اهمیت استفاده و بکارگیری و مزایای استفاده از شبکه های بی سیم بها داده نشده است. در این تحقیق سعی شده است تا حد امکان شما را با مزایا و تجهیزات و نحوه نصب و راه اندازی شبکه های بی سیم آشنا کند همچنین با پروتکل های شبکه های بی سیم نحوه رمزگذاری و امنیت آشنا خواهید شد.

شبکه های بی سیم فواید شگرفی در امر شبکه سازی بوجود آورده اند از جمله قابلیت های بسیار مفید این نوع شبکه قابل حمل بودن و آزاد بودن از محدودیت سیم ها در داخل اداره یا منزل است. اگر اداره ای از آخرین تکنولوژی شبکه، یعنی شبکه بی سیم استفاده می کند این اداره یا هر خانه ای خالی از پستی و بلندی نیست بنابراین لازم است طوری تجهیزات شبکه را چید که بهترین استفاده را از آنها برد.

اگر می خواهید یک شبکه بی سیم خانگی بدون دردسری داشته باشید بهتر است. این تحقیق را بطور کامل خوانده و از آن استفاده کنید. این تحقیق طوری طراحی شده است که در ابتدا تجهیزات مورد نیاز شبکه بی سیم را معرفی کرده و با کارکرد هر یک آشنا می شوید در گام بعدی شما را با مراحل ساخت یک شبکه بی سیم، نصب و راه اندازی، پیگر بندی شبکه و رفع اشکالات احتمالی آشنا می کند.

بعد از پایان این مطالب خواهید توانست یک شبکه بی سیم بی دردسر، سریع، امنیتی و تجهیزات فیزیکی بهینه شده درست نمائید با استفاده از شبکه بی سیم خواهید توانست در فواصل دور وظایفی را به چاپگر بفرستید و یا اینکه فایلی را به آسانی به کامپیوتر دیگری ارسال نمائید.

- 1- اضافه کردن و اشتراک گذاری تجهیزات و اتصالات اینترنتی بصورت گام به گام
- 2- رفع خرابی و افزایش قابلیت های اتصال های شبکه بی سیم
- 3- استفاده از ابزارهای امنیتی از قبیل **Firewall** و رمزگذاری داده ها و ..

این تحقیق برای کسانی که می خواهند یک شبکه بی سیم ایجاد نمایند ارائه شده است و مراحل نصب و راه اندازی آن در ویندوز 98 و **Xp** آن بطور تفصیل بیان شده است.

1- چرا شبکه بی سیم؟

در این فصل خواهیم خواند

- 1-1- شبکه های بی سیم چیستند؟
- 1-2- فواید استفاده از شبکه های بی سیم
- 1-3- سرعت واقعی شبکه های بی سیم
- 1-4- اشتراک گذاری مودم های پهن باند
- 1-5- اشتراک گذاری چاپگرها و CD و هارددیسکها
- 1-6- خلاصه فصل

شبکه بی سیم صنعت کامپیوتری است که سریعاً در حالت رشد و توسعه است. این نوع شبکه دارای تجهیزات ساده بوده و نصب تجهیزات آن آسان و قابل حمل می باشد اگر روی میز کاری شما پر از وسایل و اشیاء باشد در آن صورت فایده تجهیزات شبکه بی سیم را خواهید دید در شبکه های بی سیم نیازی به کابل کشی های طویل و دراز در اطرافها نیست و نیازی به جستجوی کابل شبکه در اتاق های کوچک که دارای کابل های فراوان هستند نخواهد بود.

اگر اداره شما از یک شبکه بی سیم استفاده می کند شما احساس خانه خودتان را خواهید داشت زیرا قادر خواهید بود در هر جا بصورت **Online** با سایر کامپیوترها و چاپگر ارتباط پیدا کنید.

با استفاده از شبکه های بی سیم می توان عملیات زیادی انجام داد که در شبکه های سیمی امکان آنها وجود ندارد یعنی سایر تکنولوژی های شبکه دارای انعطاف و قابلیت شبکه بی سیم نیستند.

به این خاطر است که استفاده کنندگان از شبکه بی سیم روز به روز افزایش می یابند اگر شخصی متصل به شبکه های بی سیم باشد محدودیتی از نظر مکان وجود ندارد یعنی شخص می تواند در هتل فرودگاه، مرکز همایش و حتی کافی شاپ و یا سایر محل ها بدون هیچ محدودیتی با سرعت خیلی بالا به شبکه بی سیم متصل شده و قابلیت استفاده از اینترنت را نیز داشته باشد بیشتر از همه موارد اصلی ترین علت عمومیت شبکه های بی سیم قابلیت در دسترس بودن در تمام ایام هفته جستجو در سوپرمارکت ها است که باعث شده طبق پژوهش شرکت **IDC** تجارت 90 میلیون دلار در سال 2001 به 60 میلیون دلار در سال 2006 برسد.

1-1-1- شبکه های بی سیم چیستند؟

منظور از شبکه سازی بی سیم در این تحقیق اتصال دو یا چند کامپیوتر و ایجاد یک شبکه محلی (**LAN**) با استفاده از امواج رادیویی جهت ارسال دریافت اطلاعات و داده ها یا اصطلاحاً سرویس انتقال می باشد. کامپیوترها در شبکه بی سیم توسط امواج رادیویی داده ها را منتقل می نمایند که این امر باعث می شود بتوان فایل ها و چاپگرها و دسترسی به اینترنت را با هر کامپیوتر موجود در شبکه به اشتراک گذاشت شما می توانید بدون قطع ارتباط با شبکه به هر اجزایی در شبکه بی سیم **LAN** رفته و استفاده نمود.

1-1-1- LAN ها ، WAN نیستند (LANs, NOT WANS)

این نکته مهم است که تفاوت بین **LAN** را با سایر شبکه های بی سیم را تشخیص دهید. شبکه های **WAN** مانند شبکه های سلولی تلفن هستند پس بنابراین وقتی درباره شبکه بی سیم صحبت می کنیم منظور ما یک شبکه خانگی است که می توانید به آن متصل شوید و تبادل اطلاعات کنید پس منظور ما فقط شبکه دیتا یا یک سلول صوتی که قبلاً آنرا **WAN** نامیدیم نیست.

برای ایجاد یک شبکه بی سیم خانگی به اجزاء اصلی زیر بنا است دو یا چند کامپیوتر که از کارت شبکه بی سیم برای اشتراک گذاری فایل ها و دسترسی اینترنت و پرینتر استفاده می کنند ممکن است یک شبکه بی سیم شامل اجزاء دیگری به شرح زیر نیز باشند:

- یک اسکنر ، هارد دیسک یا **Mp3 player** که روی شبکه **LAN** به اشتراک گذاشته شده اند.

- سخت افزار شبکه سیمی که شامل یک کابل مودم یا یک دستگاهی که بوسیله آنها کامپیوترهای وسیعی با یکدیگر در ارتباط اند که اصطلاحاً **hub** نامیده می شود

- یک **Access Point** مهمترین قسمت سخت افزاری است که به عنوان پلی بین یک شبکه بی سیم با یک شبکه سیمی بکار می رود.

در شکل 1-1 اجزاء یک شبکه محلی بی سیم ساده را به همراه اجزاء تشکیل دهنده نشان داده شده است.



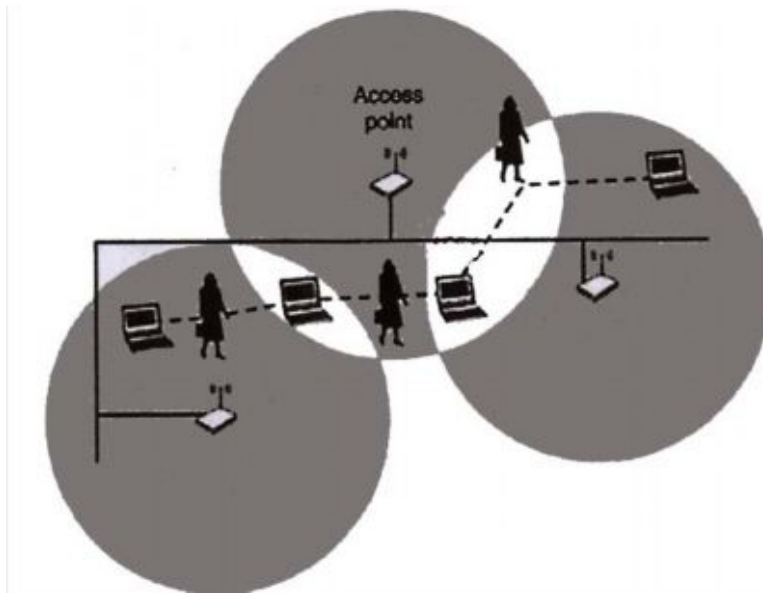
<http://www.oreillynet.com/wireless/2003/03/21/graphics/image007.jpg>

شکل 1-1

شکل 1-1: کامپیوترهایی را نشان می دهد که در یک خانه می توانند با یکدیگر با استفاده از کارت شبکه بی سیم ارتباط پیدا کنند (این کارتهای شبکه قابلیت ایجاد امواج رادیویی هستند که اصطلاحاً یک انتقال دهنده امواج رادیویی یا **transceiver** نیز گفته می شود)

با هر یک از دستگاههای شبکه بی سیم می توانید با هر یک از سلولهای شبکه ارتباط برقرار نموده و می توانید به آن داده ارسال و یا از آن داده دریافت نمائید. شبکه های بی سیم می توانند بصورت بهم پیوسته با یکدیگر ارتباط داشته باشند (شکل 1-2) در این حالت می توان یک شبکه بی سیم بزرگی ایجاد نمود و در آن اطلاعات را رد و بدل نمود که به این نوع تجهیزات اصطلاحاً **range** تجهیزات شبکه می گویند.

شکل 1-2: کاربران بدون هیچ محدودیتی در حال حرکت و تکاپو با شبکه ارتباط برقرار کنند و محدودیت تکنولوژی شبکه سیمی را ندارد.



شکل 2-1

در بقیه تحقیق انواع متفاوت تکنولوژیهای شبکه بی سیم بحث خواهیم کرد که اصطلاحاً استاندارد شبکه گفته می شود و درباره فواید و اشکالات هر یک بحث خواهد شد. مطالب این تحقیق بر روی یک تکنولوژی بی سیم متمرکز شده است عمومی ترین تکنولوژی شبکه بی سیم (یا استاندارد) برای تبادل اطلاعات بین کامپیوترها) بنام **Wi-Fi** یا **802011 b** مشهور است. تجهیزات بکار رفته در استاندارد **Wi-Fi** برای اشتراک گذاری فایلها اتصال به شبکه اینترنت و تجهیزات جانبی مانند پرینتر بزرگ است. تجهیزات **Wi-Fi** نسبتاً به سایر تکنولوژیهای شبکه بی سیم ارزان می باشد (برای اتصال به شبکه هر کامپیوتر 80 یا 100 دلار است).

2-1- فواید استفاده از شبکه های بی سیم

شبکه های بی سیم فواید زیادی ارائه می کنند که در شبکه های سیمی امکان آن وجود ندارد مهمترین و بارزترین مشخصه شبکه بی سیم قابل حمل بودن یا **portability** آن است در حالت خاص اگر کامپیوتر **laptop** را برای شبکه بی سیم تنظیم نمائید می توانید در حالت گشتن در محیط کار یا خانه و یا یک کافی شاپ از شبکه استفاده کنید.

(طولی نخواهد کشید که شاهد امکان استفاده از شبکه **wireless** در هواپیما برای دسترسی و ذخیره اطلاعات در اینترنت خواهیم بود)

- انتقال تجهیزات بطور دلخواه

درست است که شبکه بی سیم به شما اجازه خواهند داد که توسط **pool** روی صفحات اینترنت حرکت نمائید این حرف در مرکز یا جاهای کوچک صحت دارد (این در حوزه 150 متری اطراف تجهیزات خانگی بی سیم مقدور می باشد که در بخش بعدی بیشتر در این مورد بحث خواهیم کرد) عموماً ممکن است تجهیزات شبکه بی سیمی بیابید که اجازه دهد که کامپیوتر یا **laptop** را بدون خارج ساختن کابل متصل آزاد در اطراف خانه حمل نمائید پس بدیهی است که استفاده از کامپیوتر **laptop** باعث آسانی و راحتی در شبکه های بی سیم خواهد بود.

- حمل کردن کامپیوتر بی سیم در جاده

خیلی از هتل ها ، مراکز اشتغال ، فرودگاهها ، مراکز کنفرانس ها و سایر مشاغل همگی با شبکه بی سیم تنظیم شده اند که به اشخاص کمک خواهد کرد که بتواند به راحتی با سرعت بالا در مسافرت به اینترنت دسترسی داشته باشند.

بطوریکه می توان در هواپیما روی صفحات Web محتوای e-mail را مرور کرد و e-mail را چک نمود و شرکتهای Boing و sputmic و NetNearU بر روی ایجاد پهنای باندی کار می کنند که در مسافرت برای مسافران قابل دسترس باشند بعضی وقتها به آن شبکه های based – visitor یا (VBNS) می نامند این شبکه قابلیت دارند تا در هتل مراکز کنفرانس و هواپیما به اینترنت دسترسی داشته باشند.

The screenshot shows the Boingo website with a red header. The main content area features a 'BOINGO UNLIMITED' section with a price of \$9.95 per month. To the right, there are two 'Wi-Fi Plans' sections: 'LAPTOP WI-FI' for \$9.95 per month and 'MOBILE WI-FI' for \$7.95 per month. The mobile plan includes market-leading handsets and global Wi-Fi roaming. The website also has a search bar for hotspots worldwide and a footer with navigation links.

<http://www.boingo.com>

شکل 3-1

شرکت Boingo (شکل 3-1) جهت دسترسی به اینترنت بی سیم در مسافرت آداپتور شبکه b 802.11 را پیشنهاد کرده است.

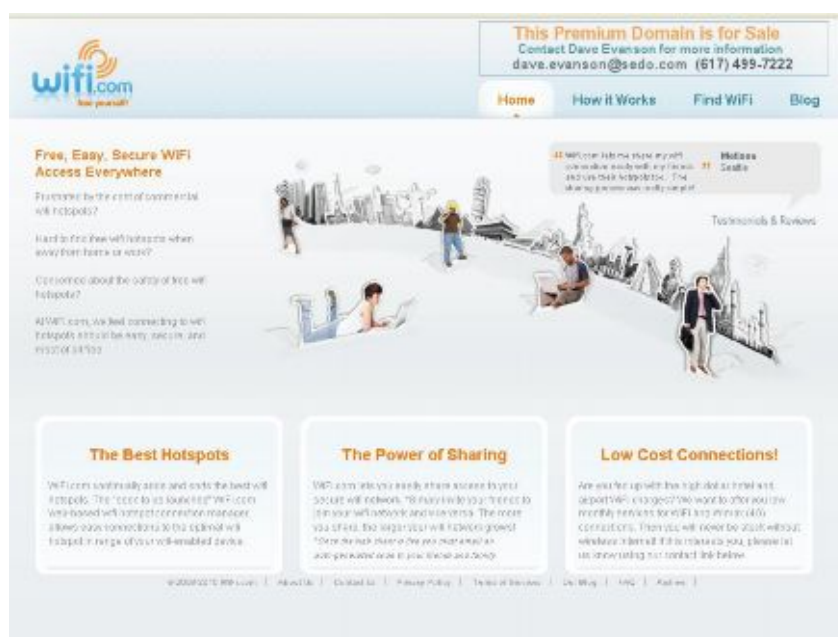
شما می توانید با مرورگر وب ها سایت [Boing\(www.boingo.com\)](http://www.boingo.com) را جستجو نمائید یا با نمونه ای از نقاط دسترسی بی سیم یا spots قبل از فصل بعدی آشنا شوید.

3-1- سرعت واقعی شبکه های بی سیم

ما دربارهٔ تکنولوژی گوناگون شبکه‌های بی‌سیم بحث خواهیم کرد در این قسمت بطور خاص در مورد سرعت آنها صحبت می‌کنیم تمام تکنولوژیها دارای یک سرعت ماکزیمم هستند که در آن سرعت می‌توانند حداکثر داده را انتقال دهند. سرعت انتقال اطلاعات به پهنای باند یا توان عملیاتی بستگی دارد. نمونه Ethernet های سریع یک تکنولوژی سیمی است که می‌توانند داده‌ها را روی کابل با سرعت 100 Mbps انتقال دهد. 802.11 a و 802.11 g سریعترین استانداردهای فعلی بی‌سیم هستند که می‌توانند ماکزیمم 54 mbps اطلاعات را منتقل نمایند. تکنولوژی 802.11 b عمومی ترین استاندارد است که می‌تواند 11 Mb اطلاعات را در هر ثانیه منتقل کند این سرعتها ماکزیمم سرعت انتقال داده‌ها می‌باشند هر چند در جهان واقعی تجهیزات شبکه‌های بی‌سیم طوری عرضه شده‌اند که قابلیت نصف سرعتها ذکر شده را دارند.

1-3-1- سازگاری و هماهنگی شرکت‌های سازنده

در این تحقیق به چکیده‌ای از تجهیزات شبکه بی‌سیم **Wi-Fi** (که آنرا با تکنولوژی 802.11 b می‌شناسید) اشاره ای خواهیم نمود. شما می‌توانید تجهیزات شبکه بی‌سیم 802.11 b را از تولید کنندگان متفاوت بخرید که باید با یکدیگر کار کنند. از کلمه «باید» استفاده کردیم زیرا ممکن است تعداد کمی از این تجهیزات با تجهیزات عمده 802.11b سازگاری نداشته باشند. برای اطمینان از سازگاری تولیدکنندگان **Wi-Fi** باید به **Wi-Fi logo** مراجعه کنید که در آن نحوه اتصال تجهیزات مورد نیاز **Ethernet** بی‌سیم سازگار بصورت متحد نشان داده شده است در (شکل 4-1) می‌توانید اطلاعات بیشتری را درباره استانداردهای بی‌سیم در سایت www.WiFi.com بیابید. شکل 4-1 مجموعه‌ای از سازگاریهای **Ethernet** بی‌سیم که گروه بازرگانی آنرا برای استاندارد 802.11 b تهیه دیده‌اند را نشان می‌دهد.



<http://www.wifi.com>

شکل 4-1

موضوع مهمی که لازم است یادآور شویم این است که **802.11 b** با استاندارد جدید (شکل 1-4) که دارای سرعت بالا و خیلی گران قیمت اصطلاحاً **Wi-Fi5** نامیده می شود کار نمی کند (یا **802.11 a**) ممکن است فکر کنید که **Wi-Fi5** از نظر زمانی 5 برابر سریعتر از تجهیزات **Wi-Fi** است در حالیکه **Wi-Fi5** قابلیت حمل حداکثر **54Mb** در هر ثانیه را دارد در حالیکه استاندارد **Wi-Fi** حداکثر سرعت **11Mb** بر ثانیه را داراست شکل 1-5 یک نقطه دسترسی یا **Point Access** از نوع **PoXim** را نشان داده است اما استاندارد جدید که **802.11 g** است از نظر سرعت شبیه **802.11 a** بوده و کاملاً با استانداردهای قدیمی سازگار بوده و اکثراً با **802.11 b** نیز کار می کند.



<http://itfanat.com/images/new-access-point---proxim-orinoco-ap-800-and-ap-8000-1.jpg>

شکل 1-5 نمونه ای از تجهیزات شبکه بی سیم **Wi-Fi5 (802.11 a)**

در شکل 1-5 تجهیزات **Wi-Fi5 (802.11 a)** از قبیل **Access Point** تولید **Proxim** دیده می شود که از نظر زمان 5 برابر سریعتر از تجهیزات شبکه بی سیم از نوع **Wi-Fi (802.11 b)** می باشد تمام استانداردهای **802.11** برای مرور صفحات **web** چاپ اسناد و گوش دادن به فایل های **mp3** سرعتهای بالایی عرضه نموده اند (یعنی اطلاع از فروشندگان لازم است به **Wi-Fi Logo** مراجعه نمائید).

4-1- اشتراک گذاری مودم های پهن باند

شاید اصطلاح دسترسی سریع به اینترنت برای طیف وسیعی از شنوندگان، تکنولوژی جدید شبکه های خانگی تلقی شود در حالیکه اصطلاح باند پهن یا **Broad Band** به تکنولوژی دسترسی سریع اینترنت از قبیل کابل و خط مشترک دیجیتالی یا **DSL** بر می گردد که انتقال داده ها به مراتب سریعتر از مودم های آنالوگ (**56 Kbps**) است مودم های کابلی دسترسی سرعت بالا بین **30** کیلوبیت تا **105** مگابیت بر ثانیه را فراهم نمودند که بروی خطوط کابل تلویزیون انجام می شد می توانید یک نمونه از مودم های کابلی از نوع **Linksys** را در شکل 1-6 مشاهده کنید ارتباط **DSL** نیز از نظر سرعت شبیه مودمهای کابلی بود با این تفاوت که در آن اصطلاحاً منظم روی خط تلفن منتقل می شدند.

شکل 1-6 یک مودم کابلی ارتباطی بمراتب سریعتر از یک مودم آنالوگ با **56** کیلوبیت بر ثانیه با اینترنت ارتباط برقرار می کند.



<http://www.hebig.org/blogs/archives/main/linksys.jpg>

شكل 1-6

هر دو ارتباط كابلى و DSL دسترسى سريع به اينترنت را عرضه مى كنند كه براى شبكه شما خيلى مفيد است ارتباط شبكه شما اگر بصورت بى سيم باشد يك ارتباط سريع به اينترنت خواهد بود بدون محدود بودن كامپيوتر به مودم.

1-4-1- پهن باند ايجاد شده توسط ماهواره

از تكنولوژى پهن باند كه خيلى كم استفاده مى شود دسترسى به اينترنت از طريق ماهواره است مانند شرκτηهاى Echo star (www.echostar.com) يا Direc Way (www.Direcway.com) اين تكنولوژى را تهيه ديده اند.

دسترسى ماهواره اى اينترنت براى گزینه هاى مانند محيط هاى روستاى بهتر است كه نمى توانند DSL يا از اينترنت كابلى استفاده كنند بنا بر اين استفاده از ماهواره نيز يك تكنولوژى بى سيم است كه شرκτηهاى فروشنده دسترسى ماهواره اى اينترنت به عنوان روشى جهت اشتراك نمودن كامپيوترهاى يك شبكه تهيه ديده اند.

استفاده از اشتراك پهن باند دسترسى به اينترنت در يك شبكه محلى داراى سه مزيت عمده است كه عبارتند از

1- شخص مقيد به خط تلفن نيست پهن باند ارتباطى اينترنت نيازى به استفاده از خط تلفن آنالوگ بمنظور استفاده از سرويس هاى اينترنتى ندارد.

2- شخص هميشه مى تواند در ارتباط باشد كه اصطلاحاً "Always on" گويند بدين مفهوم كه در اكثر مواقع ارتباط پهن باند شما بصورت Always on است بنا بر اين شخص نياز به شماره گيرى و وارد كردن نام كاربر و

رمز در هر زمانی که بخواهد به اینترنت وصل شود نیست فقط شخص لازم است که مرورگر وب خودش یا نرم افزار **e-mail** را باز کرده بصورت **online** به اینترنت متصل شود.

3- چند کامپیوتر می توانند بطور همزمان و به صورت مشترک ارتباط برقرار کنند هر شخص بطور همزمان می تواند در خانه یا اداره صفحات **web** را مرور نموده **e-mail** فرستاده و یا فایل **download** نماید. می توانید شبکه خود را بصورت **Analog** با مودم **56 Kbps** برای اشتراک کردن تنظیم نمائید اما وقتی جهت دسترسی اشتراکی به اینترنت می خواهید از شبکه استفاده نمائید بطوریکه دارای سرعت بالا باشد بهتر است از این تکنولوژی استفاده کنید.

این مزایا محدود به شبکه های بی سیم **LAN** نیستند هر چند یک شبکه بی سیم پهن باند متصل شده اینترنت از یک شبکه سیمی، خیلی انعطاف پذیرتر است و زمانیکه شما نیاز به کابل برای ایجاد شبکه نداشته باشید شما می توانید عمل اشتراک گذاری فایل ها، دسترسی به اینترنت و وسایل جانبی را بروش صحیح انجام دهید.

1-5- اشتراک گذاری چاپگرها و CD و هارددیسک ها

یکی دیگر از دلایل مفید ایجاد یک شبکه توانایی اشتراکی کردن وسایل جانبی است دو چاپگر متصل شده به یک کامپیوتر می تواند بصورت مشترک توسط تمام کامپیوترهای شبکه استفاده شود در مجموع می توان از دستگاه سخت افزار که چاپگر سرویس دهنده نامیده شد بصورت اشتراکی از یک پرینتر در شبکه استفاده نمود بدون اینکه چاپگری به **pc** متصل شود تعدادی از **Access Point** بی سیم شامل یک پورت در پشت دستگاه می باشند که بمنظور اشتراک گذاری چاپگر تعبیه شده است.

وقتی شما شبکه ای را راه اندازی می کنید می توانید هر درایوی را از هر دستگاهی را روی شبکه اشتراکی نمائید. برای مثال شخص می تواند یک نرم افزار را از روی **CD-ROM** از یک کامپیوتر رومیزی بصورت اتصال بی سیم روی **Laptop** در هر جای خانه نصب نماید یا از کامپیوتر روی میزی شخص می تواند به فایل های ذخیره شده در هارددیسک یک **Laptop** دسترسی داشته باشد فایل های موجود بر روی هارددیسک ها در یک شبکه کامپیوتری در داخل دایرکتوریها ظاهر شده همزمان در هارددیسک کامپیوتر محلی نیز قرار می گیرند منظور اینکه تمام فایل های اشتراکی توسط هر کامپیوتر متصل به شبکه در دسترس است .

همچنین شخص قادر است تجهیزات جانبی مانند **Scanner** را نیز در روی شبکه به اشتراک گذارد که برای این کار نیازه نرم افزار خاصی است مثلا شرکت **UMAX** فروشنده اسکنرهای است که برای شبکه های کامپیوتر درست شده اند که اصطلاحاً **Network-Ready Scanners** می گویند (لازم به یادآوریست اسکنرهای برای کار روی شبکه های کامپیوتری درست نشده اند) از پیشگامان چند رسانه ای که قابلیت پخش فایل های **mp3** را دارند می توان به شرکت **Panasonic** یا **Compaq** اشاره نمود در این حالت شخص می تواند آهنگ دلخواه خود را با فرمت دیجیتال **mp3** از روی هر کامپیوتر متصل به شبکه را گوش کند.

بعد از تنظیم و ایجاد شبکه بی سیم می توان بصورت عمومی از وسایل جانبی مشترک استفاده نمود که باعث صرفه جویی در هزینه می شود زیرا دیگر نیازی به خرید تجهیزات جانبی برای هر کامپیوتر بصورت جداگانه نیست. انتقال داده ها توسط نوسانات امواج رادیویی که حامل داده ها هستند قادرند در هر جا و زمانی آنها را در فلاپی ها یا **CD-ROM** ها قرار دهند.

تنظیمات یک شبکه LAN به صورت مشترک سازی فایلها و دسترسی تجهیزات جانبی روشی کاملاً مشابه در شبکه های سیم و بی سیم است و ایجاد خصوصیات چنین شبکه ای در ویندوز کاملاً ساده می باشد.

1-6- خلاصه فصل

قبل از رفتن به سراغ شبکه سازی بی سیم اگر سوالاتی برایتان در این فصل بوجود آمده می توانید بطور خلاصه جواب آنها را در اینجا بیابید.

- آیا خانه یا اداره شما برای یک شبکه بی سیم مناسب است؟ در اکثر مواقع جواب این سؤال «بلی» خواهد بود. وجود تجهیزات زیاد یک شبکه های سیمی به عنوان اشکال عمده محسوب می شود اگر خانه یا محل کار شما خیلی بزرگ باشد می توان تجهیزات شبکه بی سیم را در فاصله بیشتر 150 متر از یکدیگر قرارداد. که در این صورت لازم خواهد بود که سخت افزار شبکه بی سیم و سخت افزارهای شبکه سیمی را بطوری با هم ترکیب نمائیم در فصل 4 بطور مفصل درباره چگونگی تنظیم شبکه مرکب شامل سخت افزار شبکه بی سیم و سخت افزار شبکه سیمی (از قبیل Ethernet خط تلفن یا تجهیزات شبکه Power Line) بحث خواهد شد. گزینه ای دیگر: شما می توانید تعداد زیادی Access Point بی سیم به شبکه اضافه نمائید بطوریکه باعث شود محدوده شما یک 150 متر دیگر نیز به حوزه درونی شما افزوده گردد.

- آیا شما واقعاً نیاز به تجهیزات بی سیم دارید؟ اگر می خواهید دو یا چند کامپیوتر را در درون یک خانه یا محل کوچک به یکدیگر وصل کنید دیگر دلیلی ندارد که شما یک شبکه بی سیم ایجاد کنید در این حالت با ایجاد یک شبکه سیمی باعث صرفه جوی در هزینه و زمان خواهید بود هر چند اگر فقط یکی از این کامپیوترها Laptop باشد و بخواهید توانایی کار با آن کامپیوتر در هر نقطه ای در منزل را داشته باشید در این صورت انتخاب یک شبکه بی سیم بهترین گزینه است.

- آیا شما راضی به صرف هزینه های اضافی از نظر زمان برای نصب تجهیزات بی سیم هستید؟ با توجه به اینکه تجهیزات شبکه بی سیم خیلی انعطاف پذیرتر و قابل حمل تر از تجهیزات شبکه سیمی است بنابراین برای تنظیم و نصب آن نیز زمان زیادی لازم است منظور این است که وقتی تجهیزات شبکه بی سیم شما نصب و راه اندازی شد دیگر نیاز به خرج زمان زیاد بمنظور نگهداری آن نخواهید داشت. اگر شخصی علاقمند به انعطاف پذیر بودن شبکه بی سیم دارد پس ارزش صرف زمان زیاد را نیز خواهد داشت.

اگر شما تا کنون هیچ نوع تجهیزات را نصب نکرده اید نترسید زیرا با سرعت با نحوه درست کردن شبکه جاده بی سیم و چگونگی متصل شدن کامپیوترها و اشتراک گذاری داده ها آشنا خواهید شد. در فصل بعد چگونگی کار شبکه های بی سیم را نشان خواهیم داد و با تعدادی از اصطلاحات فنی آشنا خواهید شد و شروع به طراحی یک LAN بی سیم خواهیم نمود.

2-آماده سازی

در این فصل خواهیم خواند

1-2- آشنایی با بعضی از اصطلاحات شبکه سازی

2-2- شبکه های بی سیم چگونه کار می کنند

3-2- اشتراک سازی فایلها

4-2- اشتراک سازی اینترنت

5-2- امنیت شبکه

6-2- خلاصه فصل

برای اینکه مراحل شبکه سازی بی سیم را بهتر یاد بگیرید لازم است با تعدادی از اصطلاحات اصلی شبکه سازی آشنا شوید منظور ما این است که حتماً شما باید با تکنیک ها و دانش نحوه کار هر یک از نرم افزارها و اجزاء سخت افزارها آشنا شوید بلکه با تعدادی از اصطلاحات جدید و مفاهیم تازه که لازم است در شبکه سازی آنها را بدانند برایتان گفته خواهد شد.

تعدادی از تعاریف تکنیکی هنگام خرید تجهیزات شبکه برایتان مفهوم پیدا خواهند کرد که هنگام نیاز به پشتیبانی از طرف تولید کننده قطعات شبکه عایدتان خواهد شد.

نکته مهم دیگری که ممکن است به ذهنتان برسد این است که یک شبکه بی سیم ساده چگونه کار می کند در این فصل با نحوه انتقال داده ها در شبکه های بی سیم و همچنین با نحوه اشتراک گذاری فایل ها دسترسی به اینترنت و وسایل جانبی آشنا خواهید شد. همچنین نشان خواهیم داد که شبکه های بی سیم از نظر امنیت چگونه کار می کنند در قسمت آخر فصل باید شما درک کامل از احتیاجات ساخت بی سیم داشته باشید در پایان تحقیق عناوین زیادی وجود دارند که می توانید مطالب زیادی از آنها دریافت کرده و همچنین توصیه های زیادی درباره چگونگی نگهداری و نصب تجهیزات شبکه یاد بگیرید.

2-1- آشنا با بعضی از اصطلاحات شبکه سازی

در اینجا اصطلاحاتی وجود دارد که در سرتاسر تحقیق از آنها استفاده کرده ام زیاد نگران این نباشید که چگونه تمام آنها را در اینجا بخاطر بسپارید من آنها را در داخل متن ها معرفی خواهم کرد.

LAN (Local Area Network) یا شبکه محلی عبارتست از یک شبکه کامپیوتری که در یک موقعیت محدود قرار دارند که معمولاً این محل یک خانه یا اداره است.

Network Adaptor مبدل شبکه که اصطلاحاً به آن کارت شبکه یا کارت واسط شبکه **NIC** نیز می گویند عبارتست از یک دستگاه که بمنظور ارتباط یک کامپیوتر به یک شبکه استفاده می شود.

Access Point: (نقطه دسترسی) این دستگاه به کارتهای شبکه بی سیم امکان می دهد تا بتوانند با یک شبکه سیمی ارتباط برقرار نمایند (شکل 2-1) **Access Point** ها دارای یک جزء سیمی که همان پورت **Ethernet** و یک جزء بی سیم (یک رادیو که به کارت شبکه بی سیم امکان می دهد به شبکه کامپیوتری متصل شود) می باشد



http://images.dlink.com/new/products/DWL-2100AP/DWL-2100AP_right.png

شکل 2-1

Access Point وسیله ای است که بصورت بی سیم به منظور ارتباط دادن یک شبکه بی سیم با یک شبکه سیمی بکار می رود.

Router یک دستگاه سخت افزاری یا یک برنامه نرم افزاری است که به یک شبکه کامپیوتری اجازه می دهد تا به شبکه های دیگر متصل شود در یک شبکه محلی می توانید بوسیله یک **Router** شبکه بزرگ **LAN** خود را به یک شبکه خیلی بزرگتر مانند **Internet** وصل نمائید می توانید هنگام خرید یک **Access Point** که دارای تجهیزات **Router** نیز هست خریداری نمائید. **Router** ها به شما اجازه خواهد داد که تمام کامپیوترهای شبکه محلی شما بوسیله یک سیگنال اینترنتی مشترک به اینترنت وصل شوند.

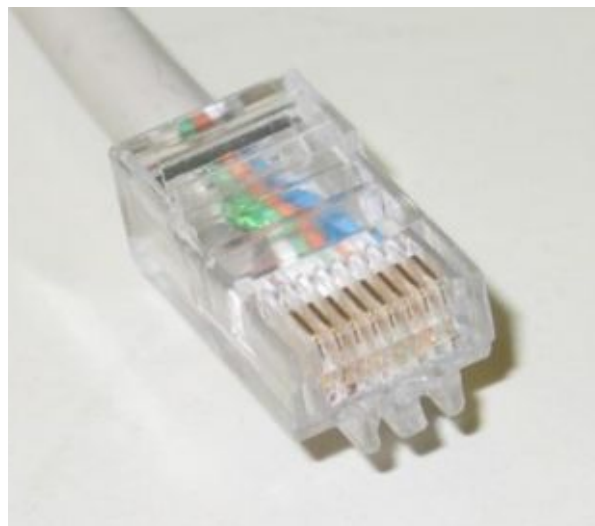
Gateway: یک **Gateway** می تواند سخت افزار یا نرم افزار باشد که اجازه می دهد تعداد کامپیوترهایی که به شکل متصل هستند را محاسبه نماید نکته مهم اینکه در یک شبکه **LAN** , **Gateway** به عنوان یک **Router** است **gateway** می تواند بوسیله یک سیگنال کامپیوتری متصل به اینترنت رابه سایر کامپیوترهای شبکه اشتراک نماید.

Protocol: پروتکل زبانی است که برای ارسال و دریافت داده ها در یک شبکه کامپیوتری استفاده می شود.

TCP/IP (Transmission Control Protocol/Internet protocol) پروتکلی است که بمنظور انتقال داده ها بر روی اینترنت استفاده می شود می توان از پروتکل **TCP/IP** برای شبکه های محلی بمنظور دسترسی اینترنت بصورت مشترک یا فایل ها یا چاپگر استفاده نمود.

Broad Band Modem (مودم پهن باند) شباهتی به مودم هایی که **56K** کیلوبیت بر ثانیه ندارد زیرا مودمهای **56Kbps** برای ارسال و دریافت اطلاعات از خطوط تلفن آنالوگ استفاده می کند در حالیکه یک مودم پهن باند سیگنالهای دیجیتالی را روی خط تلفن یا کابل **TV** ارسال می کند و قابل اتصال به **DSL** یا کابل مودم نیز است.

Ethernet یک استاندارد سیمی برای سخت افزار شبکه سازی است چرا این استاندارد به صورت تکنولوژی سیم کشی بیان کردیم تعدادی از تجهیزات از قبیل مودم پهن باند برای اتصال به **Access Point** از کابل **Ethernet** استفاده خواهند کرد (شکل 2-2) تا چندی پیش **Ethernet** تنها تکنولوژی قابل استفاده در ایجاد شبکه های کامپیوتری محسوب می شد.



<http://it.flexinet.com.au/Images/rj45.jpg>

شکل 2-2

Hub یک دستگاه سخت افزار سیمی است که به منظور اتصال چندین کامپیوتر به شبکه بکار می رود. یک **hub** دارای پورتهای 4تایی یا بیشتر است. کابلی که برای اتصال کامپیوترها به **hub** استفاده می شود مانند کابل تلفن بوده وی از آن مقدار کلفت تر است. می توان از یک **hub** برای اتصال دستگاههای سیمی مانند مودم کابلی یا **Router** به اجزای یک شبکه بی سیم مانند **Access Point** نیز استفاده نمود. اکنون با اجزاء شبکه تا حدودی آشنا شدید بطوریکه قادر هستید بهترین شبکه کامپیوتری را برای خاتمه یا اداره تان انتخاب نمائید تجهیزات مفید و سریع خریداری کنید و شبکه کامپیوترتان را با حداقل در دسر درست نمائید.

2-2- شبکه های بی سیم چگونه کار می کنند؟

کارت شبکه بی سیم جهت انتقال داده ها توسط امواج رادیویی در داخل شبکه های بی سیم روی کامپیوتر متصل می شوند اما امواج این تجهیزات شبیه امواج رادیویی حامل موج **FM** نیستند بلکه تجهیزات شبکه بی سیم تنها سیگنال های را می فرستند که فقط می توانند تا 300 متر در صورت نبودن مانع قابل استفاده باشند (این نوع عملیات معمولاً فقط در داخل حوزه 300 متری موفق به اجرا شدن هستند). در تکنولوژی شبکه های سیمی از قبیل **Ethernet** مانند شبکه های بی سیم داده ها بصورت بسته های کوچک بنام بسته های داده یا **Data Packet** منتقل می شوند هر کارت شبکه دارای یک پورت سریال منحصر بفردی می باشد که به آن اصطلاحاً **MAC (Media Access Control)** آدرس گویند. می توانید **MAC** آدرس کارت شبکه بی سیم خود را که معمولاً در قسمت پائین کارت چاپ شده مشاهده نمائید بسته های داده یا شامل داده ای که در آن آدرس فرستنده و گیرنده به همراه داده اصلی فرستاده می شوند. شبکه های بی سیم **Wi-Fi (802.11 b)** دارای تجهیزات بهتری از قبیل **g 802.11** هستند ارتباطات **Wi-Fi** از باند رادیویی 2.4 گیگا هرتز استفاده می کند آنها باند خود را با سایر وسایل الکترونیکی خانگی به اشتراک می گذارند که شامل وسایل مانند تلفن های بی سیم و ماکروویوها. شبکه بی سیم **Wi-Fi 5 (یا 802.11 a)** از باند پائین تر از **56 GHz** استفاده می کند بنابراین تاثیر خیلی کمتری از وسایل الکترونیکی خانگی می پذیرد تکنولوژیهای جدیدی مانند **Bluetooth** سریعتر از 5 زمان **Wi-Fi (شکل 2-3)** نیز عمل می کنند.



<http://static.howstuffworks.com/gif/bluetooth-card.jpg>

شکل 3-2

بطوریکه استفاده از آنها در شبکه های بی سیم رایج شده و به کاربردهای شبکه بی سیم می افزاید.

2-2-1- سایر شبکه های بی سیم

تعدادی از PDA, تلفن های Cell و Laptop ها قابلیت انتقال داده ها را با فرکانسهای خیلی بالا با استفاده از پرتوهای نورمادون قرمز را دارند. دستگاههایی که از تکنولوژی بی سیم با نورمادون قرمز استفاده می کنند اصطلاحاً IrDA (Infrarad Data Association) نامیده می شوند و می توانند با یکدیگر ارتباط برقرار کنند.

به عنوان مثال می توان یک پرونده را از یک LAPTOP به چاپگر فرستاد و از آن چاپ گرفت یا اینکه اطلاعات برخورد از یک PDA با یکدیگر را انتقال داد. IrDA یک تکنولوژی Line-of-sight است بدین مفهوم که دستگاههای استفاده کننده از IrDA در یک خط راست با یکدیگر در ارتباط هستند. Blue tooth نیز تکنولوژی دیگری است که برای انتقال داده ها از حالت بی سیم استفاده می کند. Blue tooth طوری درست شده اند که قادر هستند با PDA ها و تلفن های سلولی کار کنند و می توانند اطلاعات و داده ها را به کامپیوترهای رومیزی و Laptop ها و چاپگر انتقال دهند تجهیزات شبکه های Home RF و 802.11 b نیز همانند Blue tooth می باشد که در باند 2.4 گیگاهرتز کار می کند و نیازی به استفاده از خط راست بین اجزاء جهت انتقال داده ها در شبکه ندارند و امواج آنها می تواند از دیوار نیز عبور کنند. اکثر مواقع تکنولوژی Blue tooth به شبکه محلی شخصی یا PAN (personal Area Network) ترجیح داده می شود زیرا تکنولوژی PAN دارای محدودیت های فراوانی مانند محدودیت فاصله (مثلاً حداکثر برد 10 متر) و سرعت خیلی پائین (در حدود 720 کیلوبیت بر ثانیه) نسبت به تجهیزات بی سیم مانند 802.11 b دارند.

کارتهای شبکه های بی سیم قابلیت تبادل اطلاعات مستقیم با یکدیگر را دارند هر کارت شبکه بی سیم قابلیت ارسال و دریافت اطلاعات و انتشار داده را در داخل یک سلول را دارند یک شبکه بی سیم که در آن کارتهای شبکه بصورت مستقیم با یکدیگر در ارتباط هستند اصطلاحاً شبکه های نظیر به نظیر یا Peer-to-peer یا کار در مد ad-doc نیز گفته می شود.

شبکه های بی سیم در مد زیر ساخت یا Infrastructure نیز کار می کنند که از یک سخت افزار خاصی برای ارتباط با هر کارت شبکه استفاده می کنند که به آن Access Point می گوئیم.

2-3- اشتراک سازی فایل ها

با فعال سازی گزینه اشتراک سازی فایلها روی کامپیوترتان می توانید از هر کامپیوتر روی شبکه فایل ها اشتراکی شده را مرور با کپی نمائید سیستم عامل ویندوز دارای سرویس اشتراک گذاری فایل ها و چاپگر را در خود دارد که برای این کار لازم است فقط گزینه آن را فعال کنید.

می توانید پوشه را نیز (به همراه تمام فایل های درونی آن) به اشتراک بگذارید این کار را می توان حتی برای هر درایو سخت و یا CD نیز انجام داد. هر چند اشتراک گذاری دیسک های سخت چندان معمول نیست. هرگاه بخواهید پوشه ای را به اشتراک بگذارید لازم است با راست کلیک کردن روی آن و انتخاب گزینه **Sharing** این عمل را انجام دهید.

اگر عمل اشتراک سازی فایل های کوچک انجام دهید خواهید دید که شبکه با استفاده از تجهیزات از قبیل **802.11 a** و **802.11 g** به سرعت انجام می گیرد.

با توجه به اینکه شبکه بی سیم نسبت به شبکه های سیمی از امنیت پائینی برخوردار است لازم است در این نوع شبکه ملاحظات خاصی از نظر دسترسی افراد به منابع شبکه را در نظر بگیرند قبل از اینکه بخواهید فایلها را به اشتراک بگذارید لازم است فصل 11 تحقیق را که نحوه حفاظت داده و خصوصی سازی آنها است را بدقت بخوانید.

2-4- اشتراک سازی اینترنت

یکی از فواید اصلی و خیلی جالب شبکه های بی سیم، امکان اشتراک گذاری اینترنت است. در اینجا به نحوه کار آن خواهیم پرداخت. ارائه کنندگان سرویس های اینترنتی یا (**Internet Service Provider**) **ISP** توسط آدرس **IP** شما را شناسایی می کند **IP** آدرس یک شماره منحصر بفردی است که کامپیوتر شما را روی اینترنت شناسایی می کند.

آدرس **IP** از چهار مجموعه عدد تشکیل شده است که توسط نقطه (.) از یکدیگر جدا شده اند. این چهار عدد می تواند عددی بین 0 تا 255 باشد مانند 26.0.162.255 مشکلی که در اینجا وجود دارد این است که **ISP** قادر است فقط یک آدرس **IP** برای شما ایجاد نمایند بنابراین چگونه می توان از یک آدرس **IP** برای کامپیوترهای بیشتری استفاده نمود.

برای حل این مشکل از یک **Router** استفاده می کنند هر کامپیوتر متصل به شبکه سریعتر از اتصال مستقیم به اینترنت می توانند توسط یک نرم افزار یا سخت افزار به اینترنت متصل شوند. **Router** برای هر کامپیوتر متصل به شبکه یک آدرس **IP** مجزا تولید می کند که در کل جهان برای دسترسی به شما فقط از آن آدرس استفاده می شود با اجرای نرم افزار **Router** میتوان برای هر یک از کامپیوترها روی شبکه یک آدرس **IP** بصورت دستی تعریف نمود. برای آسودگی بیشتر بهتر است یک **Router** سخت افزاری خریداری کنید.

استفاده از **Router** سخت افزاری باعث خواهد شد که بتوانید از اینترنت بصورت اشتراکی استفاده نمائید و نیازی به منتظر ماندن صدور مجوز نرم افزاری برای استفاده از اینترنت نخواهد بود. در شبکه های بی سیم استفاده از **Access Point** که در داخل خود **Router** را نیز دارد باعث راحتی خیلی بیشتر خواهد شد این کار باعث صرفه جویی در هزینه ها و جلوگیری از مخارج اضافی خواهد شد.

2-5- امنیت شبکه

برای حفاظت اطلاعات روی شبکه چندین روش وجود دارد. برای این منظور می توانید ترکیبی از روشهای زیر را برای جلوگیری از ورود افراد ناخواسته به شبکه استفاده نمود. ما گام به گام چگونگی بکارگیری امنیت در شبکه را در فصل 11 شرح خواهیم داد در این قسمت فقط مروری سریع برای حفاظت شبکه خواهیم داشت.

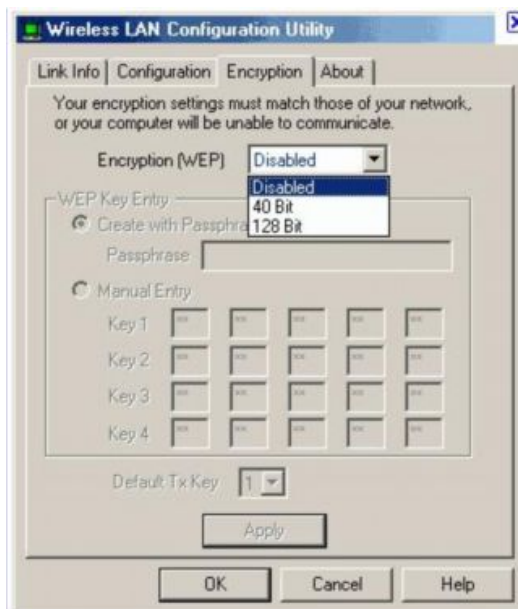
2-5-1- رمز گذاری شبکه بی سیم

سخت افزار شبکه به همراه نرم افزارهایی نصب می شوند که این نرم افزارها قادر هستند داده های شبکه را کدگذاری نمایند که این کدها برای دریافت کنندگان قابل خواندن نیستند. این داده های کد شده در مبدا توسط گیرنده در مقصد رمزگشایی می شوند استاندارد کد گذاری برای شبکه های بی سیم اصطلاحاً **Wired Equivalent Privacy (WEP)** یا (پنهان سازی مانند شبکه سیمی) نامیده می شود می توانید رمزگذاری بی سیم را توسط نرم افزاری که همراه با کارت شبکه بی سیم ارائه می شود انجام دهید.

شکل 2-4، در این شکل چگونگی فعال سازی **WEP** را روی کارت شبکه بی سیم نشان داده شده است اگر شما بخواهید این عمل را روی **Access Point** انجام دهید لازم است به فصل 11 تحقیق مراجعه کنید.

تنظیم SSID

SSID یا (**Service Set Identifier**) روی یک شبکه بی سیم نامی است که شبکه شما توسط آن نام شناسائی می شود برای دسترسی به شبکه روی هر کامپیوتر **SSID** مشابهی وجود دارد.



شکل 2-4

2-5-2- فیلترها (Filters)

2-5-2-1- (Mac آدرس)

هر کارت شبکه با سیم (و کارت شبکه سیمی) دارای یک شماره منحصر بفردی است که توسط کارخانه سازنده ایجاد شده است می توان با استفاده از آدرس MAC برای کامپیوترهای موجود در روی شبکه نحوه کار روی شبکه تعریف نمود.

2-2-5-2- دیوارهای آتش یا Firewalls

یک فایروال روی شبکه به عنوان لایه ای محافظتی است که بین شما و هکرها قرار می گیرد. فایروالها می توانند بصورت نرم افزاری روی کامپیوتر یا روی Router نصب شوند و یا اینکه از یک Standalone به عنوان دستگاه سخت افزاری فایروال استفاده نمود. با این حال با تصمیم گیری نسبت به نصب نرم افزار یا سخت افزار یک فایروال به منظور حفاظت از دسترسی افراد خارجی به شبکه استفاده می شود.

2-5-3- نرم افزارهای ویروس کش (Antivirus Software)

از نرم افزارهای ویروس کش جهت حفاظت از نفوذ و انتشار ویروس ها روی کامپیوترهای موجود در شبکه استفاده می کنیم یک ویروس می تواند بصورت مهاجم فایلها و اطلاعات موجود روی دیسک سخت را خراب نموده و به سرعت منتشر شود و در بعضی مواقع ویروسها کپی از خود را از طریق e-mail به سایر کاربران بفرستند . یک برنامه ویروس کش خوب فایل های فرستاده شده آلوده را شناسائی کرده و از انتشار آن جلوگیری می کند.

عدم بکارگیری هر یک از موارد فوق کاری ساده لوحانه است تجهیزات شبکه های بی سیم بطور ذاتی از تجهیزات شبکه های سیمی خیلی ناامن تر هستند زیرا شبکه بی سیم برای هک شدن نیازی به سخت افزار و تجهیزات فیزیکی برای وصل شدن ندارند . یک خرابکار باهوش با استفاده از روزنه هایی که پیدا می کند می تواند با استفاده از امواج هوایی به اطلاعات و داده هایتان دسترسی پیدا کند. بنابراین هر موقعی که کامپیوترتان به شبکه متصل می شود شما با یک سطح اطمینان غیر قابل اعتماد روبرو می شوید این بدین مفهوم نیست که فقط شبکه های بی سیم در مقابل هکرها شکننده هستند و نباید از آن استفاده نمود بلکه این بدان معناست که بری جلوگیری از نظرات پیش بینی نشده اقدامات امنیتی را در نظر داشته باشید. شما برای اینکه راههای نفوذ ناگهانی هکرها به شبکه کامپیوتری بی سیم را بگیریید لازم است در فصل 11 مطلب چگونگی جلوگیری از نفوذ هکرها را بخوانید.

2-6- خلاصه فصل

در این فصل خواندیم که برای راه اندازی شبکه بی سیم چه چیزهایی نیازاست . حالا می توانید از یک **Router،Access Point** و کارت شبکه در یک اداره یا یک شبکه محلی استفاده نموده و در یک روز همه آنها را راه اندازی کنید بعد از اینکه تجهیزات شبکه راه اندازی شدند می توانید فایل ها و دسترسی به اینترنت را اشتراکی کنید البته در این فصل با مفاهیم استفاده از یک **Firewall** و رمز گذاری داده ها بمنظور حفاظت داده ها از نفوذ هکرها یا هر کس دیگری که در حوزه شبکه بی سیم شما قرار دارد آشنا شدید در فصل بعد با مفاهیم چگونگی ترتیب اجزاء گوناگون در راه اندازی شبکه بی سیم **LAN** آشنا خواهید شد.

3 - ملاحظات بی سیم ها

در این فصل خواهیم خواند

3-1- مرتب سازی تجهیزات شبکه بی سیم

3-2- مد Ad-Hoc و Infrastructure (زیر ساخت)

3-3- چگونگی اثر گذاری دیوارها ، بتونها و فلزات روی سیگنالهای بی سیم

3-4- ماکزیمم سرعت و سرعت های واقعی

3-5- نحوه دریافت سیگنال کامل از Wireless ها

3-6- استانداردهای 802.11 a و 802.11 b یا 802.11 g

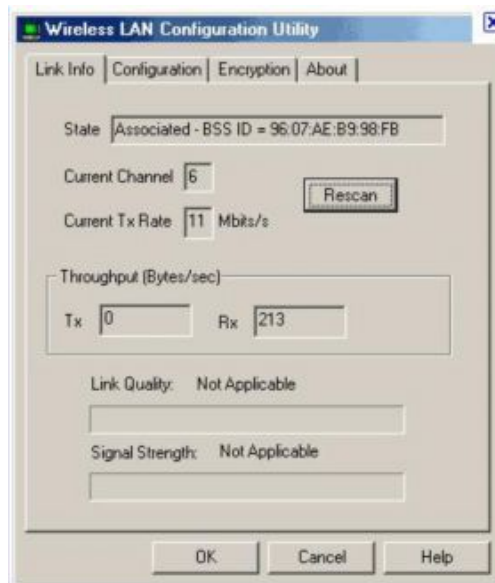
3-7- خلاصه فصل

شبکه های بی سیم نسبت به شبکه های سیمی دارای مزایای روشنی هستند که موجب محبوبیت آن شده است از قبیل شبکه اترنت و امثال آن که روی خط تلفن از طریق سیم های الکتریکی کار می کنند هر چند شبکه های بی سیم دارای معایب است.

دانستن تعدادی از عقاید موافقان و مخالفان قبل از شروع بکار شبکه بی سیم موثر است.

زمانیکه تجهیزات شبکه بی سیم روی امواج رادیویی کار می کند سیگنال ارسال از طرف شبکه فقط قادر هستند مسافت های محدودی را طی نمایند . سیگنال های شبکه بی سیم همانند امواج رادیویی قوی که قابل شنیدن در خانه یا ماشین باشند نیست بلکه امواج منتشر شده از شبکه بی سیم فقط می توانند در یک محدوده کم مانند داخل خانه منتشر شوند (این موضوع نیز در مواقعی است که هیچ مانعی در مقابل امواج نباشد) بعلاوه وقتی درباره تجهیزات شبکه بی سیم صحبت می کنیم عموماً منظور ما همان تجهیزات **Wi-Fi** (802.11 b) است که امروزه به عنوان استاندارد اصلی استفاده می شود مهمترین مانع شبکه بی سیم دریافت امواج عبور داده شده از دیوار ، آجر ، بتن ، فلزات و یک کمی نیز شیشه در فاصله های کم است . نرم افزار ارائه شده با کارت شبکه بی سیم جهت دریافت سیگنال قوی کاربران را راهنمایی خواهد کرد. نرم افزار کارت شبکه شما ممکن است کمی پیچیده تر و مشکل تر از شکل بنظر برسد اما آنها همگی دارای کارکرد یکسانی هستند.

وقتی شخص فاصله اش را از سایر کارتهای شبکه یا **Access Point** زیاد می کند نرم افزار مربوطه بطور اتوماتیک کاهش قدرت دریافت سیگنال را نشان خواهد داد و افت سرعت انتقال داده نیز نمایش می دهد



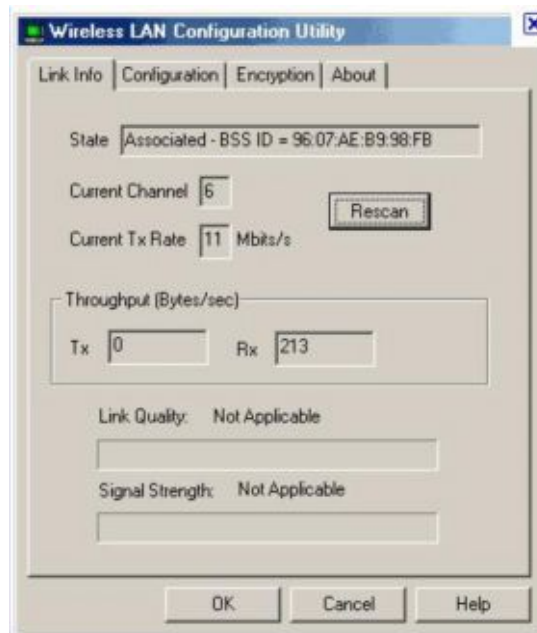
شکل 1-3

شکل 1-3 در اینجا نرم افزار کارت شبکه بی سیم در مجاورت **Access Point** نشان داده شده است در این شکل چنانچه می بینید قدرت دریافت سیگنالها 100% دیده می شود (یا حکم **Excellent** عالی) محدوده ای که می تواند امواج رادیویی شبکه بی سیم منتشر شوند **Range** نامیده می شود. **Range** یکی از مفاهیم اصلی در نحوه راه اندازی شبکه است که لازم است با آن آشنا شوید. محدودیت **Range** شبکه ها می تواند به عنوان یکی از مشکلات اساسی مطرح شود.

كاربر مى تواند به چندين روش در اين محدود كار كند براى مثال مى توان با اضافه نمودن **Access Point** به شبكه **Range** يا محدود دسترسى به شبكه را افزايش داد. همچنين مى توان با تركيب تجهيزات شبكه سيمى و شبكه بى سيم حوزه كار شبكه را افزايش داد. اين گزينه را در همين فصل شرح خواهيم داد.

3-1- مرتب سازى تجهيزات شبكه بى سيم

فرض مى كنيم كه شما يك كارت شبكه بى سيم داريد كه بر روى مادربرد كامپيوتر **Laptop** نصب شده است. شما در حال قدم زدن در اطراف خانه هستيد با افزايش فاصله شما با تجهيزات شبكه خواهيدديد كه سرعت انتقال اطلاعات در نرم افزار كارت شبكه پله پله كاهش مى يابد (شكل 3-2) با استفاده از طراحي مناسب مى توان اين كاهش را طورى نمود كه كارت شبكه بى سيم قابليت امكان اتصال مطمئن را داشته باشد.



شكل 2-3

سرعت افت انتقال اطلاعات از حداكثر سرعت **11 NGbp** تا **55Mbps** و به ترتيب 2 و 1 مگايت بر ثانيه است اگر شخص بيشتر از 150 متر دورتر برود (و يا اينكه در مسير امواج مانعى قرار داشته باشد) اين سيگنالها بيشتر ضعيف شده و ممكن است باعث قطع ارتباط با شبكه شود.

3-2- مد Ad-Hoc و Infrastructure (زير ساخت)

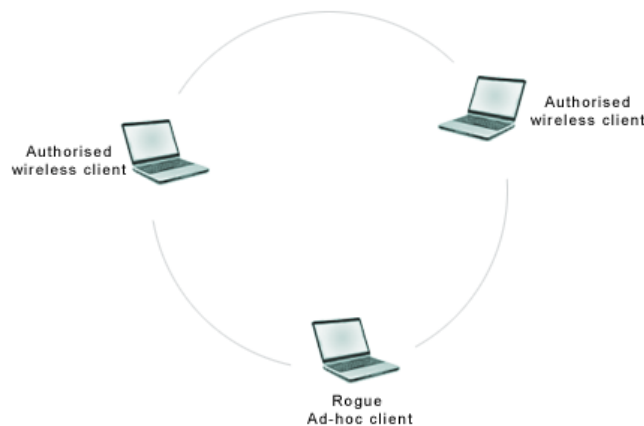
شبكه هاى كامپيوترى بى سيم نوعاً با دو نوع پيكربندى كار مى كنند (كه اصطلاحاً توپولوژى مى گويند) 1- Infrastructure-2 Ad-hoc توپولوژى يا مد روشى است كه با آن كامپيوترها مى توانند با يكديگر بصورت مستقيم يا بوسيله **Access Point** ارتباط داشته باشند.

در مد **Ad-hoc** (شکل 3-3) داده ها در شبکه توسط کارت شبکه بی سیم رد و بدل می شود توپولوژی **Ad-hoc** را اصطلاحاً شبکه نظیر به نظیر یا **peer-to-peer** نیز می گویند در اینجا تعدادی از فواید شبکه **Ad-hoc** بیان شده است.

- شبکه **Ad-hoc** دارای راه اندازی ساده است یعنی فقط لازم است کارتهای شبکه بی سیم را روی کامپیوتر نصب سپس توسط نرم افزار پیکربندی کرده و سپس اجرا نمایند.

- شبکه **Ad-hoc** ارزان قیمت و مقرون به صرفه است یعنی نیازی به خرید **Access Point** نیست و موجب صرفه جویی می شود.

- شبکه **Ad-hoc** دارای سرعت زیادی است سرعت توان عملیاتی بین دو کارت شبکه بی سیم به مراتب سریعتر از هنگامی است که بین دو **Access Point** تبادل اطلاعات می شود.



<http://www.manageengine.se/products/wifi-manager/help/alarms/vulnerability-adhoc-network-operating.jpg>

شکل 3-3

شکل 3-3: شبکه ای از نوع **Ad-hoc** بصورت مستقیم با یکدیگر در ارتباط هستند.

حال با فواید شبکه **Ad-hoc** آشنا شدیم و درک صحیحی از مزیت های **Ad-hoc** بدست آوردیم. حال برای افرادی که در خیابان یا در محل های دورتری هستند می خواهند شبکه بی سیم درست کنند چه باید کرد برای این منظور می توان محدود شبکه بی سیم را افزایش داد برای این کار لازم است یک **Access Point** به شبکه اضافه شود شبکه های بی سیم که از **Access Point** استفاده می کنند دارای مد زیر ساخت یا **Infrastructure** می باشند.

یک شبکه زیر ساخت یا **Infrastructure** دارای قابلیتهای زیر است

- قابل اتصال به یک شبکه سیمی است. **Access Point** به شما اجازه می دهد که به آسانی یک شبکه سیمی را با امکانات شبکه بی سیم توسعه دهید یعنی توسط **Access Point** می توان شبکه های سیمی و بی سیم را بهم مرتبط ساخت بطوریکه بتوانند با یکدیگر تبادل اطلاعات نمایند این مورد یکی از فواید اصلی نصب شبکه در مد **Infrastructure** است.



<http://www.pishroco.com/files/7906/Products/23860-BigPic.jpg>

شکل 3-4

شکل 3-4 یک **Access Point** از نوع **D-link** را نشان می دهد که می تواند با یک مودم کابل یا **DSL** مرتبط شود و موجب می شود تمام کامپیوترها شبکه به اینترنت دسترسی داشته باشند.

- می توانید محدود شبکه بی سیم را بسط دهید با قرار دادن یک **Access Point** بین دو شبکه بی سیم می توان محدود دسترسی به شبکه را دو برابر نمود.

- استفاده از فواید **Roaming** (در اتصالات بی سیم حرکت به آسانی و در ارتباط بودن با فرستنده بی سیم) یعنی اگر شما چندین **Access Point** رابه شبکه اضافه کنید می توان در یک اداره یا منزل بزرگ بین سلولها ارتباط برقرار نمائیم بدون اینکه ارتباط با شبکه قطع شود

- اشتراکی نمودن اینترنت: احتمالاً مفیدترین دستگاه در یک شبکه ساده بی سیم **LAN** یک **Access Point** با یک امکانات داخلی **Router** و **Firewall** باشد **Router** به شما اجازه می دهد که بصورت اشتراکی به اینترنت دسترسی داشته باشید و تمام کامپیوترهای متصل به شبکه از اینترنت استفاده نمایند همچنین وجود **Firewall** روی شبکه شما را از دسترسی کلاهبرداران حرفه ای یا هکرها حفاظت خواهد نمود تعدادی از **Access Point** های چندکاره شامل یک **hub** می باشند که توسط آن می توان چندین کامپیوتر را به شبکه **Ethernet** متصل نمود.

- آیا معایب مد **Infrastructure** را می دانید؟ نصب شبکه با مد **Infrastructure** کمی مشکل تر از حالت **Ad-hoc** است همچنین استفاده از این مد باعث کاهش سرعت انتقال اطلاعات به نصف می شود زیرا در این مد انتقال اطلاعات از طریق **Access Point** صورت می گیرد در حالیکه در **Ad-hoc** این انتقال بصورت مستقیم بین کامپیوترها بصورت می گرفت.

یکی دیگر از معایب این مد بالا بودن هزینه هاست . زیرا شبکه در مد **Infrastructure** خیلی پرهزینه تر از حالت **Ad-hoc** می باشد چون در این مد شما نیاز به خرید یک **Access Point** دارید ولی با توجه به مزایایی که قبلاً ذکر کردیم ارزش خرید یک **Access Point** نسبت به گرانی آن خیلی بیشتر است.

3-3- چگونگی اثر گذاری دیوارها، بتونها و فلزات روی سیگنال های بی سیم

انتقال امواج رادیویی در اداره یا منزل بستگی زیادی به مواد بکار رفته در دیوارها و قسمت های محیط دارد.

در اینجا مواردی ذکر شده است که لازم است در هنگام طراحی شبکه بی سیم LAN آنها را در ذهنتان داشته باشید سیگنال های کارت شبکه بی سیم برای ارسال نیاز به قرار گرفتن در یک مسیر مستقیم نیستند سیگنالهای ارسالی می توانند از بین دیوارها عبور کنند و نیازی به جهش از روی اشیاء را ندارند برای این منظور موارد زیر باید در نظر گرفته شوند

- بتونها و فلزات به شدت قدرت سیگنال ها را کاهش می دهند
- شیشه با شکست کمی از امواج باعث ضعیف شدن قدرت سیگنال ها خواهد شد
- کتاب و سایر اجسام جامد که روی میز کاری قرار دارند اگر در مسیر کارت شبکه بی سیم قرار گیرند باعث افت قابل توجهی از قدرت سیگنال خواهد بود.

تمام کارتهای شبکه بی سیم به همراه نرم افزار مربوطه ارائه می شوند که آن نحوه ارسال سیگنال های قدرتمند را نمایش می دهد اگر تجهیزات شبکه بی سیم در اداره یا منزل قرار داشته باشد با حرکت در اطراف آنها می توانید قدرت سیگنال ها را در روی صفحه نمایش ببینید این سیگنالها بصورت در صد نوشته شده بصورت نوار رنگی نمایان می گردد این رنگها هر کدام دارای مفهومی هستند اگر سیگنالها قدرتمند باشند با کلمه "Excellent" یا بصورت 100% باشد رنگ آن بصورت سبز خواهد بود. رنگ زرد بیانگر سیگنال خوب یا "fair" و رنگ قرمز بیانگر عدم ارتباط با شبکه می باشد مطالب بیشتر درباره نرم افزار مربوطه در فصل 4 بیان شده است.

3-4- ماکزیمم سرعت و سرعت های واقعی

وقتی به فروشگاه سخت افزار شبکه بی سیم مراجعه می کنید مشاهده می کنید که تمام تجهیزات ارائه شده دارای لیستی از بیشترین سرعت انتقال داده ها بصورت بسته های نرم افزاری یا روی Web Site نمایش داده می شود بنابراین لازم است صحت این سرعتها را بفهمیم.

در یک محلی که وسعت آن متوسط است استفاده از تجهیزات 802.11b که دارای سرعت بالای 11 Mbps در حالت متوسط 3-4 مگابیت بر ثانیه متداول نیست تجهیزات ذکر شده برای حالتی که دارای مودمهای کابلی یا DSL با سرعت زیاد جهت اتصال به اینترنت دارند مناسب است در محیط های کوچک مانند خانه که دارا پهنای باشند کافی است از یک کامپیوتر به منظور اتصال به شبکه اینترنت چاپگر و یا کپی کردن فایل های mp3 به سایر کامپیوترها از تجهیزات دیگری استفاده می کنند.

3-5- نحوه دریافت سیگنال کامل از Wireless ها

در محلی که شبکه بی سیم نصب شده است تضمینی در ترتیب عرض باند وجود ندارد همچنین بدیهی است که مسافت و موانع در شبکه بی سیم نیز خیلی موثر هستند (مانند بتونها و سقف ها نورافکن های خیابان ، حیوانات اطراف) در این حالت می خواهید تجهیزات شبکه را در موقعیتی قرار دهید که بتوانید

سیگنال ها را دریافت نمائید در اینجا روشهایی بیان شده است که بتواند بیشترین و قویترین سیگنال را از شبکه بی سیم دریافت نمائید

- در حد امکان محلی که تجهیزات شبکه بی سیم را در موقعیت هایی قرار دهید که در مسیر مستقیم باشند بطوریکه حداقل موانع در مسیر دریافت سیگنالها را داشته باشند تجهیزات Wi-Fi نیازی به قرار گرفتن در مسیر مستقیم ندارندولی برای کار سریعتر این شبکه نیز بهتر است آنها را نیز در مسیر مستقیم قرار دهیم.

- در صورت امکان دستگاه **Access Point** را در مسیر محلی که تجهیزات شبکه در آنجا قرار دارند نصب نمائیم.

- نصب تجهیزات اضافی شبکه سیمی در محل های آسان در فصل 4 در خصوص شبکه هایی که مرکب از مدارهای آنالوگ و دیجیتالی است بحث شده است .

- نصب **Access Point** های اضافی بمنظور توسعه محدود شبکه اگر ملاحظه کردید که شبکه شما خیلی محدود شد می توانید با نصب آنتن سیگنال های قویتر ایجاد نمائید. این آنتن ها را می توانید در محل هایی بلندتر مانند سقف محل کار وصل نمائید بطوریکه سیگنال ها دارای موانع کمتری در مسیرشان باشد لازم به توضیح است که نحوه نصب شبکه جزء مباحث اصلی این کتاب نمی باشد بهتر است بخاطر داشته باشید که خریدن یک **Access Point** دیگر بمراتب مفیدتر از خرید یک آنتن بزرگ می باشد.

3-6- استانداردهای 802.11 b و 802.11 a یا 802.11 g

بیشتر اطلاعاتی که در این قسمت قرار داده شده اند (جدول 1-3) اطلاعات جدیدی هستند جدیدتر از همه تجهیزات **WiFi5 (802.11 a)** می باشد هر چند تجهیزات **802.11 a** از نظر سرعت بر تجهیزات **802.11 b** برتری دارند (54Mbps بیشتر از 11 مگابیت است) اما کوتاه بودن حوزه فعالیت **802.11 b** از معایب آن می باشد یعنی 60 متر.

کوتاه بودن **Range** پروتکل **802.11 a** بدین معناست که نیاز به خرید **Access Point** های بیشتری نسبت به حالت **802.11 b** دارید این بدین مفهوم است که تجهیزات **802.11 a** از تکنولوژی جدیدی استفاده کرده است و از نظر قیمت نیز بمراتب گرانتر از سخت افزارهای **802.11 b** می باشد این تفاوت قیمت باعث نمی شود که شرکتها نیازی به تجهیزات شبکه های بی سیم با سرعت بالا نداشته باشند اما برای مکانهای کوچک مانند خانه ، خرید تجهیزات **802.11 b** توصیه می شود.

جدول 1-3 خصوصیات 802.11 a، 802.11 b و 802.11 g

ملاحظات	کاربردها	رنج تقریبی	حداکثر سرعت
دارای سرعت خیلی پائین نسبت به 802.11 a یا 802.11 g	بهترین نوع برای اشتراک گذاری فایل‌های اینترنت و چاپگر	150 m	11Mbps
دارای سخت‌افزار خیلی گران قیمت نسبت به 802.11 b دارد	کمترین تداخل امواج بین تلفن های بی سیم و دستگاههای Blue tooth دارد زیرا از باند 2.4 Gh استفاده می کند	60m	54 Mbps
تکنولوژی جدیدی که دارای قیمت زیادی است قابلیت تحمل دستگاههای الکترونیکی که باند 2.4 GH کار می کنند را دارد مانند تلفن های سلولی	سریع و قابلیت سازگار بودن با تجهیزات 802.11 b	تقریباً 10% کمتر از 802.11 b است	54Mbps

اکثر افرادی که از شبکه خانگی استفاده می کنند ترجیح می دهند که از سخت‌افزار شبکه بی سیم ارزان قیمت از نوع 802.11 b استفاده نمایند. این نوع شبکه باید مرور صفحات وب، اشتراک گذاری فایلها و چاپگرها بسنده نمایند. اما در شبکه های اداری که نیاز به اتصال به Laptop دارند (قابلیت حرکت و اتصال به شبکه را دارند) اکثراً از تجهیزات 802.11 g و 802.11 g که استفاده می کنند این نوع شبکه ها نیازمند به سرعت زیاد جهت کپی فایل های بزرگ از قبیل بانکهای اطلاعاتی تصاویر گرافیکی و فایل های ویدیویی دارند.

7-3- خلاصه فصل

قبل از اینکه شروع به ساخت بی سیم نمائیم لازم است با فاکتورهای محدود کننده تجهیزات شبکه بی سیم آشنا شوید در خانه های خیلی بزرگ یا محل کار با وسعت بیشتر نیازمند به نصب تجهیزات اضافی از قبیل سخت افزارهای شبکه سیمی یا **Access Point** های اضافی دارد تا بتوان یک سیگنال قوی با اتصالهای سریعتر به سخت افزار شبکه بی سیم ایجاد نمود برای این منظور به تجهیزات جدیدی که دارای سرعت بالا دارند روی آورند. این تجهیزات شامل پروتکل های **802.11 g** و **802.11 a** می باشد این تجهیزات دارای ویژگیهایی از قبیل کوتاه بودن ساخت قیمت خیلی بالا، قابلیت ترکیب با تجهیزات شبکه بی سیم **802.11 b** قدیمی می باشند و عموماً برای نصب شبکه در خانه یا اداره استفاده می شوند.

4- نصب سخت افزار و نرم افزار شبکه

- در این فصل داریم
- 1-4- گزینه های اتصال
- 2-4- نصب سخت افزار
- 3-4- مرور نرم افزار
- 4-4- استفاده از مد **Ad-hoc**
- 5-4- کار با **Access Point** ها
- 6-4- رفع عیب یا **Trouble shooting**
- 7-4- نحوه قرار گرفتن تجهیزات
- 8-4- ایجاد شبکه **peer-to-peer**
- 9-4- نحوه ساخت یک شبکه ابتدایی
- 10-4- تنظیمات از دستگاههای چند رسانه ای شبکه
- 11-4- ترکیب نمودن تجهیزات 802.11
- 12-4- خلاصه فصل

این فصل، فصل جالبی است در این فصل شما با استفاده از فصول گذشته شروع به نصب سخت افزارهای شبکه بی سیم خواهید نمود بنابراین در این بخش شما فقط به دو کامپیوتر نیاز دارید یا اینکه می توانید کامپیوترهای زیادی را در اداره پیکربندی نمائید. در اینجا یاد خواهید گرفت که چگونه کامپیوترها با یکدیگر تبادل اطلاعات می نمایند. پیچیده ترین قسمت ایجاد یک شبکه بی سیم در این فصل نحوه ارتباط کارتهای شبکه با یکدیگر خواهد بود لذا بهتر است تجهیزاتی را خریداری نمائید که نصب و راه اندازی آنها آسانتر است به عنوان مثال استفاده از **Access Point** های دارای **Router** داخلی.

4-1- گزینه های اتصال

سه گزینه اصلی جهت انتخاب کارتهای شبکه بی سیم وجود دارد با توجه به استاندارد اتصال شبکه بی سیم و نوع کامپیوترهای مورد استفاده جهت ایجاد شبکه گزینه های زیر را انتخاب می کنید این گزینه ها عبارتند از یک کارت ، **pc** ، **USB** یا کارت **PCI** اجازه دهید نگاهی به تفاوتهای بارز کارتهای شبکه داشته باشیم (جدول 1-4).

جدول 1-4 کارتهای شبکه انتخاب شده برای **WiFi**

آنگاه استفاده کنید از	برای استفاده با	اگر دارید
کارت PC	Laptop	802.11b
USB	کامپیوتر رومیزی	802.11 b
کارت PC	Laptop	802.11 a یا 802.11 g
کارت PCI	کامپیوتر رومیزی	802.11 a یا 802.11 g

کارت **pc** اسلاید کارتهای **pc** (شکل 1-4) در یکی از دو **slot** موجود روی **laptop** قرار می گیرند باید توجه داشت که اسلات کارت **pc** اکثر بنام اسلات **PCMCIA** شناخته می شوند (**PCMCIA** مخفف **personal Computer Memory Card International Association**) کارت شبکه های بی سیم **pc** برای **Notbook** ها بزرگتر هستند بنابراین کارت شبکه **laptop** ها کوچک بوده و نصب آنها نیز آسان است. وقتی شما در جاده هستید می توانید کارت **pc** نصب شده روی **laptop** را خارج نمائید می توان از کارت شبکه بی سیم **USB** (شکل 2-4) نیز روی **Laptop** بکار برد هر چند کارت **USB** فضای زیادی را بعلت استفاده از یک حلقه سیم اشغال می کند و این چندان خوشایند نیست.



http://www.mrgadget.com.au/blogimages/belkin_pre-n_wireless_notebook_network_card.jpg

شکل 1-4



http://www.productwiki.com/upload/images/netgear_wgr614l.jpg

شکل 2-4

1-1-4-1-کارت های USB

برای اتصال کامپیوتر رومیزی به یک شبکه 802.11 b استفاده از USB بهترین گزینه انتخابی خواهد بود. کارت شبکه USB (Universal Serial Bus) ارزان قیمت بوده و بسادگی قابل نصب می باشد. PC هایی که در محیط windows 98 یا بالاتر کار می کنند نوعا نیازمند به دو پورت USB دارند این پورت ها hot-swappable هستند یعنی می توان این تجهیزات را بدون Reboot کردن سیستم نصب یا خارج نمود. این بدین مفهوم است که در اکثر مواقع هنگام نصب نیازمند به راه اندازی مجدد کامپیوتر به منظور سازماندهی نرم افزار کارت شبکه می باشد.

موردی که باید هنگام استفاده USB در شبکه بی سیم باید در نظر گرفت این است که آنرا در شبکه های 802.11a و 802.11g نمی توان بکار برد زیرا USB دارای سرعت کافی جهت حمل داده ها در این

شبكه هاى بى سيم ندارد زيرا سرعت اين شبكه ها 54Mbps مى باشد در حاليكه حداكثر انتقال اطلاعات 12Mbps, USB مى باشد.

4-1-2- کارت هاى PCI

کارتهاى PCI (Peripheral Component Interconnect) (اجزاء جانبى اتصال داخلى) اکثر جهت اتصال کامپيوترهاى روميزى به شبكه بى سيم بكار مى روند نصب يک کارت PCI روى کامپيوتر مراتب حرفه اى تر از نصب يک کارت شبكه USB مى باشد زيرا هنگام نصب کارت شبكه PCI نياز است که Case کامپيوتر باز شده و کارت شبكه PCI روى يکى از Slot هاى آزاد در داخل آن نصب گردد اين عمل کار خطرناک و پيچيده اى نيست اما زمان زيادى مى گيرد مخصوصا موقعى که با يک کارت شبكه USB مقايسه مى شود در اوایل کارتهاى شبكه PCI در حالت 802.11b وقتى نياز به نصب روى کامپيوتر داشتند لازم بود آنها را در داخل يک کارت شبكه pc ديگرى نصب مى کردند براى يادآورى بهتر است به جدول 2-4 نظرى کوتاه داشته باشيد.

4-2-2- نصب سخت افزار

اکنون قدمهاى اصلى نصب يک شبكه بى سيم رابرايتان نشان خواهيم داد. بايد به خاطر داشت که تجهيزات خريدارى شده براى راه اندازى شبكه ممکن است داراى دستورالعمل نصب در خود بسته فروخته شده موجود باشد که خيلى بهتر و منظم تر باشد بنابراین لازم است به دستورالعمل هاى ارائه شده به همراه تجهيزات نظرى داشته باشند.

در اينجا ايده سريعى از فرايند کار را برايتان بيان مى کنيم.

1- نصب کار شبكه

2- نصب درايورهاى کارت شبكه

3- راه اندازى مجدد کامپيوتر

فروشندگان سخت افزار در اکثر موارد توصيه هاى را جهت نصب نرم افزار کارتهاى شبكه ارائه مى کنند وجود اين نرم افزارها هنگام خريد خيلى مهم است زيرا ممکن است تجهيزات سخت افزارى خريدارى شده به غير از نرم افزار مربوطه قابل استفاده نباشند.

4-3-3- مرور نرم افزار

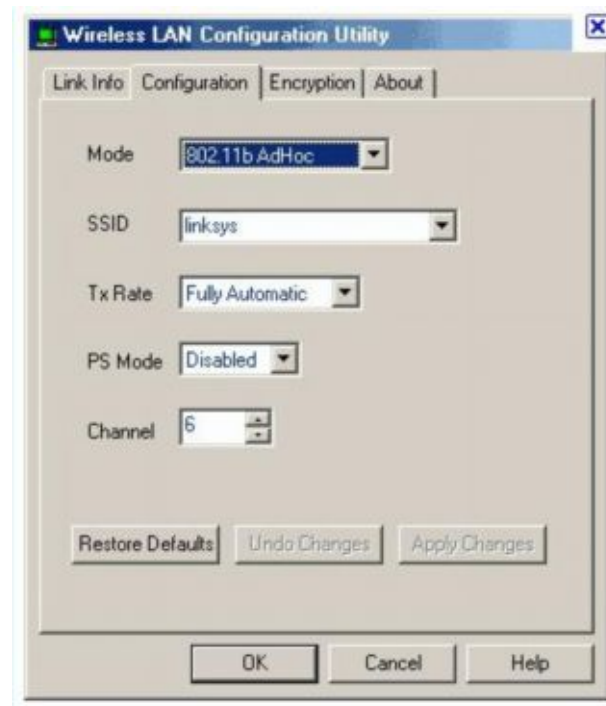
برای شروع استفاده از تجهيزات شبكه بى سيم نياز به هر نرم افزار خاصى نخواهيد داشت با استفاده از نرم افزا ارائه شده به همراه کارت شبكه بى سيم به سرعت مى توانيد يک ارتباط بى سيم دو کارت شبكه (در حالت ad-hoc) يا Access Point ايجاد نماييد. (در حال Infrastructure).

نصب 3 نرم افزار در راه اندازى شبكه و ايجاد ارتباطى خيلى مهم است اگر هر يک از اين موارد بدرستى روى کارت شبكه يا Access Point نصب و تنظيم نشوند شبكه شما کار نخواهد کرد اين 2 مورد عبارتند از Mode يا حالت SSID و WEP.

ابتدا بوسیله نرم افزار ارائه شده عمل پیکربندی را انجام دهید (در حقیقت در اکثر مواقع هنگام نصب pc روی کامپیوتر بصورت اتوماتیک ویندوز یک حالت پیش فرض را انتخاب می کند) ولی بهتر است از نرم افزار ارائه شده استفاده نمائیم.

1- یعنی ابتدا نرم افزار نصب شبکه بی سیم که به همراه سخت افزار ارائه می شود یعنی Wireless LAN configuration utility را باز می کنیم.

2- از منوی Configuration یکی از حالت های Ad-hoc یا Infrastructure (شکل 3-4) را انتخاب می کنیم قبلاً توضیح دادیم که اگر تجهیزات شبکه بی سیم بصورت مستقیم به کارت شبکه بی سیم متصل شوند حالت Ad-hoc و اگر با استفاده از Access Point این عمل صورت گیرد حالت Infrastructure را انتخاب می کنیم.



شکل 3-4

3- SSID یا (Service Set Identifier) یا مجموعه سرویس شناسایی نامی است که برای شبکه در نظر گرفته شده است باید از SSID برای نام گذاری وسایل سخت افزاری یا تجهیزاتی که قادر به اتصال به شبکه نخواهند بود استفاده کنیم.(شکل 4-4)

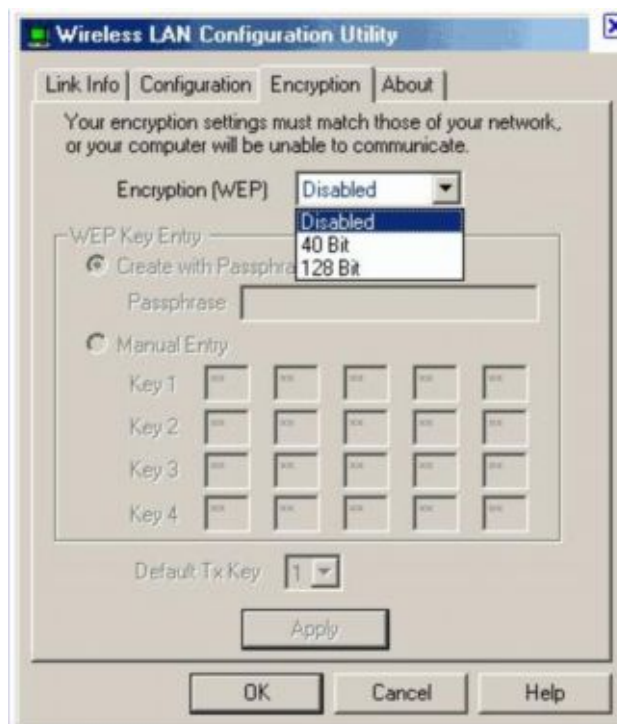
SSID می تواند به راحتی هکرها را شناسائی نماید که می خواهند بوسیله نرم افزار "sniff" از طریق امواج هوایی به شبکه نفوذ کنند بنابراین SSID به عنوان محافظ از نفوذ کاربران غیر مجاز که در داخل محدود شبکه هستند جلوگیری می کند.



شکل 4-4

شکل 4-4: اگر برای SSID گزینه "ANY" انتخاب شود در این صورت کلیه کارتهای شبکه در 2.11 b80 می توانند به شبکه دسترسی داشته باشند.

از منوی **Encryption** (رمز گذاری) **Enable** یا **Disable** کردن **WEP** (شکل 4-5) را می توان انجام داد. با استفاده از این منو می توان رمز گذاری شبکه بی سیم را تنظیم نمود یعنی این گزینه باعث می شود کلیه تجهیزات شبکه بی سیم یکدیگر را شناسایی کنند تمام کارتهای شبکه و **Access Point** ها لازم است دارای **wep** در حالت های **on** یا **off** باشند در غیر این صورت تجهیزات شما قادر به اتصال به شبکه یا ارتباط با یکدیگر نخواهند بود (شکل 4-5).



شکل 5-4

با تنظیمات بیان شده روی کلیه تجهیزات باید کامپیوترها آماده ارتباط با شبکه باشند ممکن است بخواهید بعضی از خصوصیات شبکه را بوسیله **Windows** نصب شده روی کامپیوترها تغییر دهید تا بتوان فایل ها را به اشتراک گذاشت این موضوع نیز در فصل 6 و 7 به طور کامل شرح داده شده است.

4-4- استفاده از مد Ad-Hoc

نصب و راه اندازی شبکه در مد **Ad-hoc** می توان به عنوان روشی سریع و ارزان در طراحی اولیه شبکه ها استفاده نمود در اینجا مراحل ضروری برای نصب و راه اندازی سخت افزار در مد **Ad-hoc** بیان شده است

1- نصب کارت شبکه روی سیستم

2- نصب درایو کارت شبکه

3- راه اندازی مجدد کامپیوتر

4- پیکربندی نرم افزار در حالت **Ad-hoc**

بعد از راه اندازی یکی از کارتهای شبکه بی سیستم بیسیم این عملیات را روی تمام کامپیوترهایی که می خواهید به شبکه متصل شوند را انجام دهید در این حالت چند کامپیوتر می تواند به شبکه متصل شود **Ad-hoc** حداکثر می توان 256 کامپیوتر را به شبکه متصل نمود.

توجه :

کارتهای شبکه بیسیم می توانند به سرعت توسط باتری کامپیوترهای **laptop** تغذیه شوند. در مواقعی که به شبکه بی سیم متصل نیستند و یا اینکه در مسافرت هستید و مدت زیادی به شبکه متصل نخواهید شد کارت شبکه از باتری داخلی کامپیوتر استفاده می کند بنابراین بهتر است کارت شبکه بی سیم را از کامپیوتر **laptop** جدا کنید.

بخاطر داشته باشید اگر بخواهید در حالت **Ad-hoc** از اینترنت بصورت اشتراکی استفاده نمائید نیاز به نرم افزار اشتراک سازی ارتباط (**Connection Sharing Software**) از قبیل **Internet Connection sharing** یا **(ICS)** که در سیستم عامل **win 98 SE** و بعد از آن مانند **2000, windows Me** و **xp** ارائه شده است خواهیم داشت بنابراین جهت استفاده کلیه کامپیوتر از اینترنت کافی است یکی از کامپیوترها به اینترنت متصل شود.

4-5- کار با Access Point ها

استفاده از **Access Point** روشی خیلی مفیدی جهت توسعه شبکه بی سیم می باشد در این حالت امکان اتصال به شبکه های سیمی و یا اشتراک گذاری مودم پهن باند نیز وجود دارد.

راه انداز ی **Access Point** خیلی آسان است برای منظور کافی است آداپتور تغذیه برق را به پریز برق وصل نموده و سپس با استفاده از کابل **Ethernet** آنرا به کامپیوتر یا **hub** متصل نمائید کار با **Access Point** ها کاری مهارتی به نظر می رسد بنابراین لازم است قبل از شروع به کار با **Access Point** مقداری از تواناییها و کاربردهای آن اطلاعات کسب نمائیم.

در کل دو نوع **Access Point** اصلی وجود دارد.

Access Point-1 هایی که به عنوان پل بین شبکه بی سیم و شبکه های سیمی بکار می رود.

Access Point -2 هایی که در آنها **Router** نیز تعبیه شده است این **Router** باعث می شود که تمام کامپیوترهای موجود در شبکه به صورت اشتراکی به اینترنت دسترسی داشته باشند.

بعد از اینکه توانستید تمام تغییرات مورد نیاز برای نصب و راه اندازی **Access Point** با استفاده از دستورالعمل ارائه شده به همراه تجهیزات را انجام دهید در این حالت شما آماده راه اندازی آن خواهید بود از تنظیمات ذکر شده به عنوان نمونه می توان به تنظیم رمزگذاری یا **SSID** که قبلاً ذکر شده اشاره کرد.

توجه: باید توجه داشت که کلیه **Access Point** ها قادر به ایجاد ارتباط با یکدیگر نیستند بنابراین لازم است **Access Point** هایی خریداری کنید که بتوانند با یکدیگر ارتباط برقرار نمایند (که اکثراً بنام **Ethernet over point** یا **Ap-to-Ap** نامیده می شوند) این نکته در بکارگیری **Access Point** های متعدد در خانه یا اداره همچنین توسعه شبکه و ارتباط با شبکه های سیمی خیلی سودمند می باشد بنابراین اگر شما چنین هدفی دارید لازم است قبل از خرید **Access Point** تمام خصوصیات آنها را بررسی نمائید.

می توان **Access Point** هایی خریداری نمود. که در داخل آنها **Router** و **hob** به منظور اتصال سیمی کامپیوتر ها به **Router** تعبیه شده است در بخش بعد با نحوه راه اندازی بهتر و مفیدتر آن آشنا خواهیم کرد.

4-5-1- Access Point های دارای Router داخلی

اگر قبلاً برای شبکه **Router** خریداری نکرده اید تاکیداً **Access Point** هایی که به همراه **Router** ارائه شده اند توصیه می گردد زیرا **Access Point** به تنهایی قادر به اشتراک گذاری اینترنت نیست لذا با صرف هزینه ای اندک اضافی می توان صاحب **Router** و **Access Point** شد اگر بخواهید تنها **Access Point** نصب نمائید سپس برای اتصال به شبکه سیمی (**Ethernet**) یک **Router** جداگانه نصب نمائید. این کار ممکن است کمی گرانتر باشد بنابراین بیش از یک اتصال انجام دهید و مراحل نصب شما خیلی زیاد گردد. لازم به ذکر است که اکثر موارد به **Router** دروازه یا **Gateway** نیز می گویند یک **Gateway** اصطلاحی وسیع می باشد که از نرم افزار و سخت افزار تشکیل شده است و امکان دسترسی به اینترنت را برای کامپیوتر های شبکه ممکن می سازد.

اکثر **Router** ها زمانیکه به شبکه وصل می شوند بوسیله مرورگر **web** پیکربندی می شوند هنگام استفاده از مرورگر **web** می توان به سادگی آدرسی به آن داد عموماً بصورت 192.168.0.1 هر **Router** باید دارای خصوصیت **NAT** باشد (**Network Address Translation**) اجازه می دهد که یک آدرس **Ip** را که توسط (**Internet Service Proviser**) تهیه شده بصورت اشتراکی بکار برید **NAT** یک سری از زیر آدرسهاست (**sub Address**) که در شبکه بکار می رود این آدرس های **Ip** در محدوده 192.168.0.1 تا 192.168.0.255 می باشد و در روی اینترنت نشان داده نمی شوند این کار به دو دلیل انجام می شود.

1- كامپيوترهاى شما از ديد هكرها و كسانيكه ممكن است بخواهند به سيستم شما دسترسى پيدا كنند مخفى مى ماند.

2- با استفاده از يك آدرس IP مى توانيد تعداد زيادى از كامپيوترها را به اينترنت وصل نمائيد در اين حالت فقط يك كامپيوتر به عنوان استفاده كننده از اينترنت نشان داده مى شود و آن نيز آدرس IP مربوط به IP مى باشد بنا بر اين نياز به خريد آدرس هاى IP متعدد نيستند.

بعد از اينكه Router نصب گرديد با باز كردن مرورگر web مى توانيد دستگاه را پيكربندى نمائيد ممكن است با تنظيمات بر روى ISP از قبيل وارد كردن نام كاربر و رمز عبور طورى عمل كنيد كه نخواهيد هر كامپيوترى به ISP متصل شود سازندگان سخت افزار يا ISP لازم است دستورالعمل پيكربندى را نيز تهيه و ارائه نمايند اكثر نمونه هاى Router براى اتصال آماده و تنظيم شده اند و به صورت پيش فرض قابل استفاده هستند.

در اينجا سه مرحله اصلى تنظيم يك Router بيان شده است

1- مرورگر وب را باز كنيد

2- يك آدرس IP به Router تان اختصاص دهيد

3- مسير آنرا از طريق ISP دنبال كنيد ممكن است آدرس IP قبلاً داده شود در اين حالت شما از تنظيمات پيش فرض استفاده کرده ايد كه به ISP يك آدرس IP اختصاص مى دهد.

در قسمت هاى بعدى تحقيق ساير خصوصيات Router جهت استفاده بهتر بيان شده است از قبيل قابليت انتخاب يك كارت شبكه به منظور دسترسى به شبكه و جلوگيرى از ملحق شدن سايرين به شبكه و كنترل دسترسى كاربران.

توجه:

تعدادى از ISP ها مخصوصاً تهيه كنندگان دسترسى به اينترنت كابلى براى هر كامپيوتر كه مى خواهيد به اينترنت وصل شود هزينه اى دريافت مى كنند بايد يادآور شد كه به منظور دسترسى به اينترنت پهن باند ISP از يك Router استفاده مى كند اگر ISP مانع استفاده اشتراكى Router از آدرس IP شود اين عمل از طريق تهيه كنندگان انجام شده است.

براي نمونه اگر شركت كابل محلى اجازه استفاده از Router را ندهد مى توان سرويس DSL را خريدارى نمود.

4-6- رفع عيب يا Troubleshooting

بعد از اينكه تمام تجهيزات شبكه بى سيم شما متصل شدند ممكن است كارت شبكه هاى وجود داشته باشند كه هنوز ارتباط برقرار نكرده اند اگر در روى كارت شبكه شما چراغ سبى روشن باشد مفهوم آن اين است كه كارت شبكه شما با Access Point درمد Infrastructure و يا با ساير كارتهائى شبكه در مد Ad-hoc در ارتباط است.

مراحل عیب یابی عبارتست از:

- 1- تست کردن connection ها
- 2- مطمئن شدن از اینکه تمام تجهیزات در مد Ad-hoc تنظیم شده اند (در صورت نبودن Access Point).
- 3- مطمئن شدن از اینکه مودم کابلی یا DSL کار می کند و به ISP متصل است بعضی از مودمها دارای 3 چراغ هستند و باید همه آنها روشن باشد.

4-7- نحوه قرار گرفتن تجهیزات

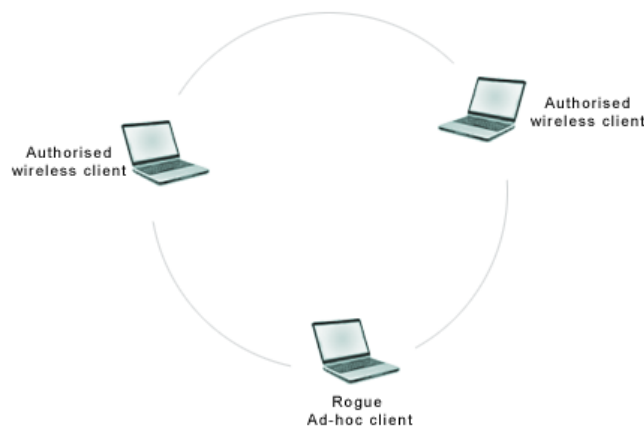
محل قرار گرفتن تجهیزات شبکه خود بحث مهمی است و به شما یک ایده بصری در خصوص چگونگی مرتب سازی تجهیزات به منظور بهره گیری از حداکثر حوزه فعالیت و استفاده مفیدتر از شبکه بی سیم ارائه می کند در اینجا درباره چگونگی قرار گرفتن تجهیزات برای دو کامپیوتر شبکه بی سیم بحث می کنیم برای اینکه این کامپیوترها با یکدیگر قویترین سیگنالهای داده را رد و بدل کنند بهتر است بصورت مستقیم همدیگر را ببینند. در شبکه هایی که چندین کامپیوتر را می خواهیم شبکه کنیم چند کامپیوتری مانند ادارات لازم است شبکه را طوری طراحی کنیم که هم از تجهیزات شبکه سیمی و بی سیمی به نحو احسن استفاده نمائیم.

4-8- ایجاد شبکه peer-to-peer

فرض می کنیم که شما فقط دو کامپیوتر دارید که نیازی به اتصال به اینترنت ندارند (شکل 11-4) و یا اینکه با اشتراکی کردن دسترسی به اینترنت فقط در یکی از کامپیوترها سایر کامپیوترها نیز قابلیت اتصال به اینترنت را داشته باشد در این حالت بهترین انتخاب شبکه نظیر به نظیر یا peer-to-peer است شبکه peer-to-peer دارای دو مزیت است اول اینکه ارزان قیمت است دوم اینکه نصب و راه اندازی آن آسان است در این نوع شبکه فقط لازم است روی هر دو کامپیوتر کارت شبکه بی سیم نصب گردد. اصلی ترین عیب شبکه peer-to-peer محدود بودن مسافت عملکرد امواج رادیویی است که هر کارت شبکه از خود منتشر می کند برای رفع این مشکل نیاز است که شبکه را در حالت Infrastructure توسعه دهیم که در قسمت بعد به آن خواهیم پرداخت.

4-9- نحوه ساخت یک شبکه ابتدایی

فرض می کنیم می خواهیم فایل ها و چاپگرها را بین بیش از دو کامپیوتر به اشتراک بگذاریم و همچنین می خواهیم با استفاده از یک مودم پهن باند دسترسی به اینترنت را اشتراکی نمائیم در این حالت استفاده از شبکه Infrastructure بهترین انتخاب خواهد بود.



<http://www.manageengine.se/products/wifi-manager/help/alarms/vulnerability-adhoc-network-operating.jpg>

شكل 4-6

نصب و راه اندازى شبكه **Infrastructure** كمى مشكلتر از شبكه **Ad-hoc** است اما نصب آن زمان زيادى را نمى گيرد با اين حال در مجموع فوايد شبكه **Infrastructure** بيشتر است. وجود **Access Point** در اين شبكه باعث ارتباط دستگاههاى سيمى با دستگاههاى بى سيم از قبيل مدمهاى كابلى، شبكههاى سيمى در شبكههاى داخلى ادارات شده و باعث توسعه شبكه به اندازه مورد نياز خواهد شد.

4-9-1- تنظيمات يك شبكه پيوندى

فرض مى كنيم در محلى كامپيوترهاى روميزى داريم كه قابليت حمل تجهيزات سخت افزارى آنها مشكل است و استفاده از كارتهاى شبكه بى سيم كامپيوتر **Laptop** مفيدتر است در چنين حالتهاى مى توان تكنولوژى سيمى و بى سيم (**no- new-technologies**) را تركيب نمود. از قبيل خط تلفن و خطوط انتقال نپرو كه در سيم كشى ساختمان بكار رفته است اين تكنولوژيها در مراكز الكترونيكى يا ادارات قابل استفاده هستند.

يعنى مى توانيد به تجهيزات شبكه برق و خطوط تلفن با استفاده از **Access Point** بى سيم و كارت شبكه متصل شد.

نصب و راه اندازى شبكههاى دوگانه ممكن است مشكل به نظر برسد با اين حال تنها شبكه اى است كه قابليت كار و توسعه در اكثر محيطها از قبيل ادارات و خانه هاى بزرگ كه در آن وسايل سيمى مانند تلفن و امكانات الكترونيكى وجود دارد را داراست اما اين شبكه خيلى بزرگ بوده كه يكى از معايب شبكههاى بى سيم به حساب مى آيد.

4-10- استفاده از دستگاههاى چند رسانه اى شبكه

موضوع مى خواهيم به يك شبكه بى سيم يك دستگاه كه مستقلاً كار مى كنند مانند **Mp3 player** يا **Printer server** اضافه نماييم.

نیازی نیست که تمام دستگاهها و تجهیزات به یک کامپیوتر متصل شوند می توان از دستگاههایی استفاده نمود که سرعت شبکه شما را تسریع نماید از قبیل **Printer server** بی سیم که نیازی به اتصال فیزیکی به شبکه ندارد همچنین می توان از دستگاههایی که هر کس استفاده می کند مانند اسکنر یا **Mp3 player** که به آسانی می توانند به **Access Point** که دارای **Port** هایی برای **hub** دارند متصل شوند. در بخش بعد شرح خواهیم داد که چگونه می توان تجهیزات قدیمی را در امکانات جدید شبکه بکار برد و به نوعی شما را در بالا بردن سرعت عناصر شبکه راهنمایی خواهیم نمود.

4-11- ترکیب نمودن تجهیزات 802.11

فرض می کنیم شما دارای تجهیزات شبکه **WiFi** هستید و سرمایه زیادی به آن خرج کرده اید در این هنگام در مغازه ای به تجهیزات جدید شبکه بی سیم برخورد می کنید و جذب آن می شوید. در این حال نیازی به دور ریختن سخت افزار قدیمی نیست شما می توانید تمام تجهیزات سخت افزاری شبکه قدیمی را با تجهیزات جدید وفق داده و از صرف هزینه اضافی صرفه نظر نمایند.

اگر شما یک **Ethernet hub** به شبکه اضافه کنید می توان بیش از یک **Access Point** به این **hub** وصل نمود که به عنوان پلی بین پروتکل **802.11 a, 802.11b** و شبکه **Ethernet** عمل می کند. و تکنولوژی جدید بی سیم مانند سخت افزار سریع شبکه **802.11 b** که در آن عملیات با سرعت **22Mbps** انجام می شود و یک تکنولوژی که دارای قابلیت سازگاری به سخت افزار قدیم را دارد مانند تجهیزات **802.11 g** با سرعت **11Mbps** قرار دارد.

در آینده با تکنولوژیهای جدید بی سیم برخورد خواهیم کرد که ممکن است با تجهیزات قدیمی کار کنند و یا خیر. اما برای اطمینان خاطر از کارکرد شبکه می توان تجهیزات مفیدتر و سریعتر را در آینده خریداری نمود یا اینکه با اضافه کردن یک **hub** یا سخت افزار **Backward-compatible** نیازهایتان را برطرف نمائید.

4-12- خلاصه فصل

می خواهید چه نوع شبکه ای بسازید؟ این مطلب به تعداد کامپیوترهایی که می خواهید متصل شوند بستگی دارد. شبکه های **Ad-hoc** فقط امکان متصل شدن دو کامپیوتر به یکدیگر را می دهند اما شبکه های **Infrastructure** باعث توسعه شبکه با استفاده از **Access Point** می شود شبکه های دوگانه یا **Hybrid Network** امکان ترکیب کردن تکنولوژیهای سیمی و بی سیم را فراهم می کند شبکه ها با دستگاههای مستقل **Standalone** باعث ایجاد امکانات سودمند و جالب بودن متصل شدن سخت افزار به کامپیوتر می شود.

5- ایجاد شبکه با استفاده از استانداردهای بی سیم

در این فصل داریم

1-5- یک شروع خوب 802.11 b

2-5- شبکه سازی بی سیم بصورت PDA

Home RF-3-5

4-5- حرکت به سوی 802.11 a

5-5- پدیده ای نو 802.11 g

6-5- ارسال فایل ها از طریق اشعه مادون قرمز

7-5- چاپ از طریق اشعه مادون قرمز

8-5- خلاصه فصل

اکنون زمان انتخاب بهترین نوع تکنولوژی شبکه سازی بی سیم برای خانه یا LAN اداره رسیده است در این فصل با تکنولوژیهای جدید شبکه های بی سیم که باعث افزایش سرعت و بهره وری خواهد شد آشنا خواهیم شد و همچنین مزایای هر یک از شبکه های بی سیم را از نزدیک لمس خواهیم کرد. زمانیکه می خواهیم نسبت به خرید و نصب استاندارد **802.11 b** اقدام نمائیم بهتر است با سایر استانداردها شامل **802.11 a** و **802.11 g** نیز آشنا شویم و با مزایا و معایب هر یک قبل از خرید تجهیزات آشنا خواهیم شد.

5-1- یک شروع خوب برای **802.11 b**

ارزانی و قابل اطمینان بودن استاندارد **802.11 b** می تواند به عنوان شروع خوبی برای شبکه سازی باشد بهره وری (سریعتر از اتصال به اینترنت) و سادگی از خاصیت این نوع استاندارد می باشد. با اینحال استاندارد **802.11 b** تنها تکنولوژی شبکه سازی بی سیم نیست و سایر تکنولوژیهای شبکه سازی بی سیم با استاندارد **802.11 b** عموماً مفید تر نیز هستند می توانید با استفاده از اشعه مادون قرمز به **laptop** و **PDA** ها متصل شد و یا اینکه از یک **Laptop** چاپ بگیرید. استاندارد **802.11 b** چندان در تمام مکانها شایع نشد به همین علت نیز ما در این فصل به سایر تکنولوژیها خواهیم پرداخت با این حال در بخش بعد با استفاده از **802.11 b** نحوه اتصال یک **PDA** به شبکه را نشان خواهیم داد.

5-2- شبکه سازی بی سیم بصورت **PDA**

حال با توجه به اینکه با شبکه بی سیم کار می کنیم می توان با حذف کابل **USB** یا کابل سریال پورت یک **PDA** بصورت بی سیم به کامپیوتر متصل شد و به **E-mail** یا **Address book** دسترسی داشت. فرض می کنیم یک قرارداد تجاری معروف از یک ساحل بوسیله **fax** ارسال شده است اکثر **PDA** ها امکان ارتباط با اینترنت را ندارند برای این مشکل لازم است یک مودم بی سیم (یا به کابل سریال متصل شده و سپس به خط تلفن) خریداری نمائید. تمام **PDA** با سیستم عامل **pc packet** یا **palm** کار می کنند و قابلیت **synch** داده را دارند این به این معنی است که می توانید روی یک دکمه فرمان کلیک کنید اصطلاحاً **cradle** گویند (یا انتخاب گزینه استفاده از نرم افزار) با این عمل می توانید داده ها را از **pc** به **PDA** منتقل نموده و یا برعکس عمل کنید با این روش تمام داده های شما به **PDA** یا کامپیوتر منتقل می شوند اکثر **PDA** ها قابلیت انتقال داده بصورت بی سیم در مسیرهای کوتاه را دارند اما آن کافی نیست ممکن است کامپیوتر دستی شما از یک اشعه مادون قرمز استاندارد که قابلیت شناسائی اکثر **laptop** نیست استفاده نماید و یا اینکه اکثر کامپیوترهای رومیزی قابلیت اشعه مادون قرمز را ندارند. قابلیت های بی سیم موجود روی **PDA** اکثر برای تبادل داده ها بین **PDA** ها مفید است و این کار زمانی مقدور است که در **PDA** شبیه به هم که از نور مادون قرمز همانند استفاده می کنند در دسترس باشد. بنابراین چگونه می توان در شبکه از **PDA** بصورت بی سیم استفاده نمود در این موقع است که استاندارد **802.11 b** بکار می رود می توان با خرید یک کارت اضافه **802.11 b** برای **PDA** این عمل را انجام داد.



<http://ecx.images-amazon.com/images/I/41iaYg%2BIHiL.jpg>

شکل 1-5

به عنوان مثال می توان یک آداپتور از نوع **SMC, Ohink, Netgear** و .. برای **PDA** (شکل 1-5) خرید با طی مراحل زیر می توان به شبکه بی سیم متصل گردید.

1- نصب درایور کارت شبکه

2- نصب کارت شبکه بی سیم روی **PDA**

3- شروع بکار **PDA** طبق دستورالعمل کارت شبکه برای اتصال به شبکه

به محض اینکه وارد محدود شبکه بی سیم شدید **PDA** شما آماده ورود به شبکه است در مجموع هماهنگی روی شبکه بی سیم به **PDA** امکان خواهد داد که بتوانند صفحات وب را مرور کرده و **E-mail** دریافت نمایند. همچنین در زمان هائی که به اینترنت وصل نیستند خواهید توانست صفحات **web** را دانلود کرده و آخرین **e-mail** را مرور نمائید در یک کلام اینکه **b 802.11** یک استاندارد است که برای استفاده بیشتر و مفیدتر از **PDA** ها بکار می رود.

Home RF-3-5

یک استاندارد رقیب برای **b 802.11** است با این تفاوت که این استاندارد قابلیت چند رسانه ای دارد هر چند شرکتهای تولید کننده **Home RF** اخیراً درصدد توقف تولید این محصول هستند استاندارد شبکه سازی بی سیم می تواند از تلفن های بی سیم استفاده نماید این مورد زمانی اتفاق می افتد که از باند 2.4 **GHZ** که تلفن های بی سیم بکار می روند استفاده نمایند در مجموع **Home RF** وسیله ای دستی است که قابلیت اجرای فایل های صوتی و تصویری مانند **Mp3** را دارد این استاندارد با توجه به قابلیت انتقال فایل های چند رسانه ای دارای اولویت باشد.

بنابراین سوال این است که چرا هر کس از **Home RF** استفاده نمی کند؟ خط پائین **b 802.11** قبلاً توسط شرکت تولید کننده به باند پهن تنظیم شده است که قابلیت شنوایی را در ادارات و خانه های بزرگ ایجاد می کند اما نکته مهم این است که **b 802.11** سرعت بیشتری را ارائه می کند.

اولین نسخه های **Home RF** با سرعت **1Mbps** کار می کرد که این سرعت برای مرور صفحات **web** بد نبود ولی این سرعت برای اشتراک گذاری فایل ها خیلی پائین بود اولین نسخه **802.11** (وابسته به **802.11 b**) سرعت **2Mbps** را ارائه نمود دومین نسخه **802.11 b** (با سرعت **11Mbps**).

5-4- حرکت به سوی **802.11 a**

همواره یک اعتراض ثابتی درباره شبکه های بی سیم وجود داشت و آن پائین بودن سرعت آن بود این اعتراضات چندان طول نکشید تجهیزات **802.11 a** اکنون بطور گسترده در دسترس است و یک سرعت ماکزیمی در حدود نصب **Fast Ethernet** ارائه می کند (**100Mbps**).
تجهیزات **802.11 a** مخصوصاً برای شرکت هایی خوب است که کاربران نیاز به تکنولوژی سریع توسعه شبکه سیمی توسط **Access Point** را دارند (شکل 2-5) قیمت تجهیزات **802.11 a** تقریباً 2 برابر تجهیزات **802.11 b** می باشد که برای اکثر کاربران خانگی استفاده از آن خوشایند نیست. اکنون تنها کارتهای شبکه **Laptop**ها دارای این تکنولوژی هستند و کامپیوترهای رومیزی چنین کارتهای شبکه ای را ندارند.



<http://www.pishroco.com/files/7906/Products/23860-BigPic.jpg>

شکل 2-5

همانند تجهیزات **802.11 b** می توان با استفاده از **Access Point** سخت افزار شبکه سیمی و بی سیم را ترکیب نمود. برای نمونه می توان با یک **Access Point** شبکه **802.11 a** یک مودم کابلی را اشتراک سازی نمود همچنین می توان یک **Access Point** را به یک **Hub** متصل کرد بطوریکه بتوان از آن برای چند منظور استفاده نمود برای مثال با اتصال **hub** به خطوط تلفن یا خطوط برق یک شبکه سیمی و بی سیم را مخلوط نمود بطوریکه بتوان به سادگی تمامی اتاقهای خانه به شبکه دسترسی داشته باشند.
در قسمت بعدی آخرین استاندارد **802.11** که دارای سرعت بیشتر و سادگی شبکه سازی را داراست آشنا خواهید شد.

5-5- پدیده ای نو بنام 802.11 g

استانداردهای شبکه بی سیم 802.11 a و 802.11 b ناسازگار بودند یعنی به فرض اگر شما شبکه ای با استاندارد 802.11 b داشتید و می خواستید آنرا به 802.11 a ارتقا دهید ممکن بود کارتهای شبکه استاندارد جدید را جایگزین استاندارد قدیم می نمودید یا اینکه می توانستید عملگرهای دوشبکه بی سیم را نگهدارید که با سرعتهای متفاوت با هم کار می کنند.

در استاندارد ذکر شده دارای محدوده های دسترسی متفاوتی هستند با وجود سرعت بالای 802.11 a دارای محدود دسترسی یا range کوتاهترین نسبت به 802.11 b بود (حدوداً 60 متر).

اما تکنولوژی جدید 802.11 باعث متحد شدن دو استاندارد گردید.

این تکنولوژی جدید 802.11 g بود که مانند 802.11 a با حداکثر سرعت 54Mbps کار می کند با این تفاوت که این استاندارد در باند 2.4GHz عمل کرده و این امر باعث سازگاری آن با 802.11 b شد.

در جدول 5-1 تعدادی از سایر استانداردهای شبکه سازی را مشاهده می کنید که می توانید در آن فواید و معایب هر یک را مشاهده کنید

استاندارد	سرعت	مزیتها	معایب
Home RF	10Mbps	قابلیت صوتی و تصویری	سریعتر از 802.11b نیست و نمی توان بصورت طولانی استفاده کرد
802.11b	11Mbps	ارزان بودن - قابلیت دسترسی به صورت همزمان و در هر مکان	از سایر تکنولوژیهای بی سیم کندتر است
802.11a	54Mbps	سرعت بیشتر	با استاندارد 802.11 b ناسازگار است
802.11g	54Mbps	سازگار با 802.11b است دارای محدود وسیعتر از 802.11a است	از سایر تکنولوژیهای 802.11 خیلی گران قیمت تر است

این استاندارد نیز مانند 802.11 از تکنولوژی متناوبی RF (فرکانس رادیویی) برای انتقال ساده فایلها بین دو کامپیوتر استفاده می کند تکنولوژی اشعه مادون قرمز از یک پرتو نوری برای ارسال داده ها بین توان کامپیوتر را سریعتر به یکدیگر متصل نمود و بین آنها فایلها را ارسال و دریافت نمود.

5-6- ارسال فایل ها از طریق اشعه مادون قرمز

لازم به یادآور است که اشعه مادون قرمز (IR) یک تکنولوژی Line-of-site است یعنی در این حالت لازم است تجهیزات شبکه شما در موقعیتی قرار داشته باشند که بتوانند بصورت مستقیم در دید یکدیگر باشند و تبادل اطلاعات نمایند. اشعه مادون قرمز قادر به عبور از دیوارها و کف اتاقها نیست در حالیکه تکنولوژی فرکانس رادیویی مانند 802.11 b این قابلیت است.

برای ارسال داده ها بین دو کامپیوتر نیاز به یک پورت اشعه مادون قرمز که عموماً روی اکثر Laptop ما وجود دارد یا اینکه می توان آنرا روی سیستم اضافه نمود.

نکته:

توجه داشته باشید این استاندارد را که **(Infrared Data Association) IrDA** می نامند در اکثر **laptop** و **PDA**ها استفاده شده است اکثر **palm os PDA** از تکنولوژی دیگر اشعه مادون قرمز استفاده می کنند بنابراین نوع تکنولوژی اشعه مادون قرمز در تبادل داده ها و چاپ مهم می باشد.

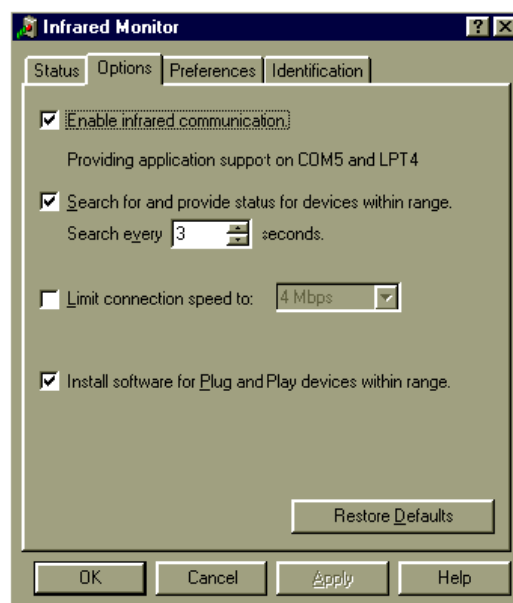
در اینجا نحوه انتقال داده بین دو کامپیوتر که ویندوز با استفاده از نرم افزار اتصال کابل مستقیم (**Direct Cable Connection**) در داخل ویندوز 98 نشان داده شده است ابتدا لازم است قابلیت اشعه مادون قرمز (**Infrared**) را روی **Laptop** یا سایر دستگاههای بی سیم که می توانند با این اشعه کار کنند فعال نمایند.

برای این کار مراحل زیر را انجام می دهیم

1- از **Infrared Control Panel** روی **Infrared** دوبار کلیک می کنیم.

2- روی گزینه **Option** کلیک کرده و گزینه **Enable Infrared Communication** را فعال می کنیم.

بخاطر داشته باشید پورتی که قابلیت کار با اشعه مادون قرمز را دارد در زیر این گزینه نشان داده خواهد شد (شکل 4-5)



http://www-307.ibm.com/pc/support/site.wss/lwik-3vjll8_4.gif

شکل 3-5

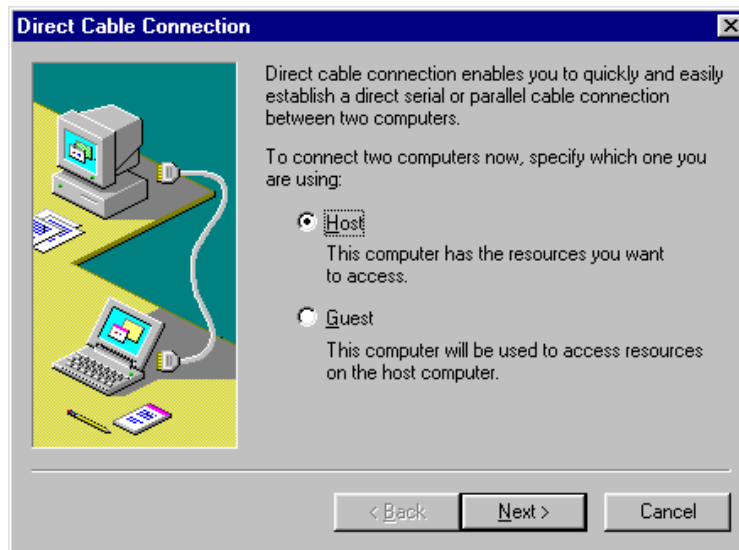
3- گزینه **Start → Program → Accessories → Communication** را انتخاب نمائید.

4- سپس گزینه (**Direct Cable Connection**) را انتخاب کنید اگر این پنجره را ببینید ممکن است نیاز به نصب آن از **CD** ویندوز داشته باشید برای اینکار مراحل زیر را طی کنید. (شکل 5-5)

Start → setting → Control Panel → Add Remove Programs

سپس روی کلید **windows setup** کلیک کنید سپس گزینه **Communication** را انتخاب نمائید و در داخل آن روی گزینه **Direct cable Connection** علامت 3 بگذارید.

5- پنجره Direct cable connection Wizard ظاهر مى شود.



شكل 5-4

در اين مرحله از شما خواسته مى شود كه از کدام پورت استفاده مى كنيد كه انرا در قسمت 1 يعنى windows enable ظاهر مى شود با طى اين مراحل يك ارتباط بى سيم مادون قرمز با ساير كامپيوتر برقرار خواهد شد.

در ويندوز XP قابليت Infrared به طور پيش فرض روى كامپيوتر توسط Infrared transceiver فعال مى شود با ترتيب قرار دادن Laptop دوربين ديجيتالى يا PDA اين دو دستگاه خواهند توانست در يك متری از يكديگر ارتباط مادون قرمز برقرار نمايند.

بعد از كامل شدن مراحل ارتباطى يك آيكون در task Bar ظاهر شده كه بيانگر امكان ارتباط مى باشد. بنابر اين با استفاده از نور مادون قرمز مى توان بين يك PDA و Laptop داده رد و بدل نمود اما اشعه مادون قرمز داراى پهنای كمى است كه در مقايسه با 802.11 b خيلى كندتر است لذا بهتر است از استفاده آن منصرف شويد.

5-7- چاپ از طريق اشعه مادون قرمز

چاپ كردن بى سيم بدین معنی است كه اتصال به چاپگر در اطراف آن و بدون اتصال سیمی به چاپگر چاپ مقدور است به این مفهوم نیست كه در مسافرت بتوانید با Laptop به چاپگر در محل كار متصل شويد و عمل چاپ انجام دهید برای چاپ از طريق اشعه مادون قرمز نیاز به موارد زیر است

- يك اشعه مادون قرمز روى كامپيوتر

- يك پورت دریافت كننده اشعه مادون قرمز روى چاپگر

چاپگرهاى Inkjet توليدى شركت Hewlett Packards (HP) اكثر شامل پورت مادون قرمز مى باشند با اينحال اكثر چاپگر داراى اين پورت نیستند برای حل این مشکل مى توانيد پورتى مانند كامپيوتر را برای نصب روى چاپگر خريدارى نماييد.

5-8- خلاصه فصل

اگر چه امروزه بصورت گسترده از **802.11 b** به عنوان استاندارد شبکه بی سیم استفاده می شود اما سایر استانداردهای مفیدی وجود دارد که می توانید به سادگی به یک شبکه بی سیم متصل شوید استاندارد **802.11 a** به عنوان یک روش سریع در شبکه بی سیم معرفی گردید ولی این استاندارد با **802.11 a** به عنوان یک روش سریع در شبکه بی سیم معرفی گردید ولی این استاندارد با **802.11 b** سازگار نبود تکنولوژی اشعه مادون قرمز نیز می تواند برای ارتباط کامپیوترها و چاپگرها استفاده شود اما این تکنولوژی خیلی کندتر از **802.11b** است و قابلیت عبور از دیوارها را ندارد تکنولوژی جدید **802.11 g** تکنولوژی خیلی سریع است که قابلیت سازگاری با تکنولوژی های قدیم (**802.11b**) را نیز دارد و این امر باعث حذف مشکل ناسازگاری خواهد شد.

6- آموزش گام به گام شبکه سازی در ویندوز 98

در این فصل داریم

1-6- اطمینان از شناسائی سخت افزار

2-6- تست کردن برای **TCP/IP**

3-6- نام گذاری کامپیوتر و گروه کاری

4-6- شروع اشتراک گذاری فایل ها و چاپگر

5-6- استفاده از شبکه مجاور یا **Network Neighborhood**

6-6- دسترسی اشتراکی به اینترنت بصورت بی سیم

7-6- خلاصه فصل

ابتدا لازم است این سوال از شما پرسیده شود که آیا روی کامپیوتر شما سیستم عامل **windows** وجود دارد اگر جواب مثبت باشد شما دارای شانس خوبی هستید زیرا در این فصل ما نحوه نصب و راه اندازی شبکه بی سیم در سیستم عامل ویندوز 98 را به شما یاد خواهیم داد. کامپیوترهایی که روی آنها سیستم عامل ویندوز 98 نصب شده است به آسانی قابل شبکه شدن هستند در مجموع اکثر نسخه های جدید ویندوز از قبیل **XP** و 2000 بصورت پیش فرض روی شبکه نشان داده می شوند در فصل بعد نحوه نصب شبکه بی سیم روی این سیستم عامل ها را نشان خواهیم داد. تفاوتی فاحش بین ویندوز 95/98 و ویندوز **Me** وجود دارد در ویندوز **ME** جدید اکثر نوآوریهای شبکه بصورت **wizard** قرار داده شده است که می توان بصورت دستی روی آن تغییرات انجام داد در مجموع می توان گفت ویندوز **ME** دارای امکانات شبکه (**Network Place**) می باشد یعنی در آن توسط پوشه ای می توان به منابع شبکه دسترسی پیدا کرد در حالیکه ویندوز 98 و 95 دارای خاصیت همسایگی شبکه یا **Network Neighborhood** می باشد.

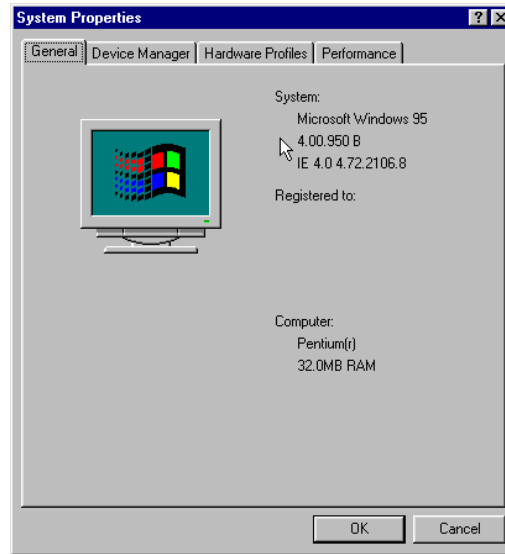
6-1- اطمینان از شناسائی سخت افزار

بعد از نصب قطعات سخت افزار روی کامپیوتر لازم است آنها را از نظر تشخیص توسط سیستم عامل بررسی نماییم این عمل با استفاده از گزینه **Device Maneger** صورت می پذیرد.
1- روی **My Computer** موجود در **Desktop** راست کلیک کرده و گزینه **properties** را انتخاب کنید. (شکل 6-1)



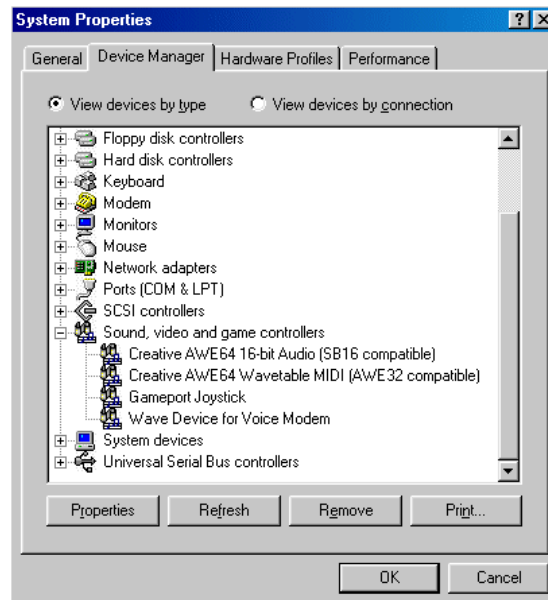
شکل 6-1

2- روى نشانه **Device Manager** كليك كنيد. (شكل 2-6)



شكل 2-6

از ليست دستگاهها روى **Network adaptor** دو بار كليك كنيد. (شكل 3-6)



شكل 3-6

اگر در داخل اين گزينه کارت شبكه بى سيم مشاهده نكرديد بايد از اتصال صحيح آن روى كامپيوتر اطمينان حاصل كنيد اگر از اتصال سخت افزارى آن اطمينان حاصل كرديد لازم است درايو آنرا مجدداً نصب نمايئد. اگر تجهيزات شما توسط سيستم عامل تشخيص داده شد كامپيوتر شما آماده دسترسى به اينترنت است در غير اينصورت لازم است تعدادى نرم افزار كه امكان ارتباط شما با هر كامپيوترى كه به اينترنت وصل شده روى كامپيوترتان نصب نمايئد.

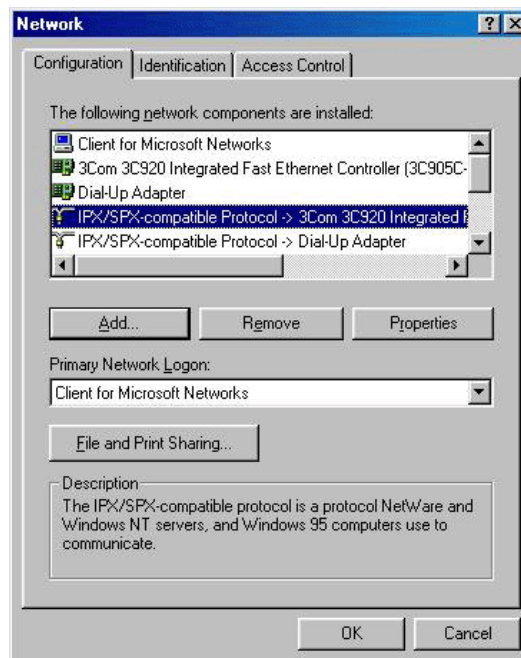
6-2- تست کردن برای TCP/IP

ابتدا لازم است مطمئن شوید که آیا پروتکل TCP/IP روی کامپیوترتان وجود دارد یا خیر. اینترنت دسترسی داشته باشید و فایل ها را اشتراکی نمایید. TCP/IP (Transmission Control Protocol/Internet Protocol) به شما امکان می دهد که به کامپیوترها روی اینترنت با آن زبان گفتگو می کنند در شبکه داخلی می توان از TCP/IP به دو منظور استفاده نمود یکی اشتراکی کردن فایل ها روی اینترنت و دوم اشتراکی نمودن چاپگرها.

حال اجازه دهید مراحل نصب TCP/IP (در صورت نبودن روی سیستم عامل) را برایتان آموزش دهیم.

1- CD سیستم عامل را در CD-ROM قرار دهید

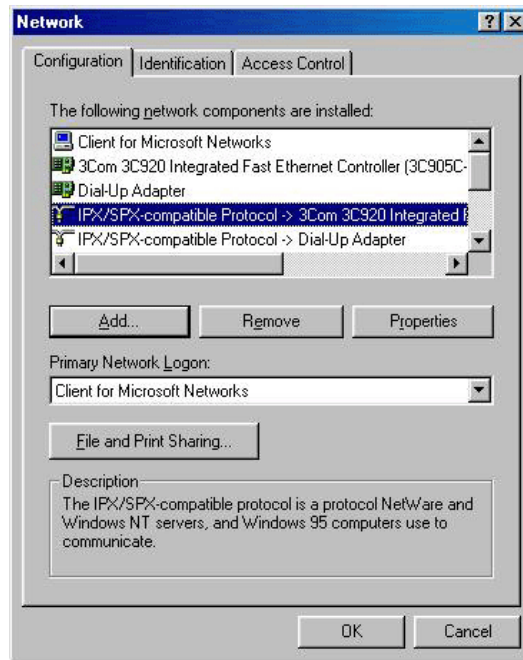
2- از Desktop روی گزینه Network Neighborhood راست کلیک کرده و گزینه Properties را انتخاب کنید. (شکل 4-6)



شکل 4-6

3- از پنجره ظاهر شده در قسمت "The Following Network Components are Installed" لازم است نام کارت شبکه ای که در Device Manager نشان داده شده در لیست مذکور ببینید مفهوم آن این است که کارت شبکه شما نصب گردیده است همچنین در این لیست باید پروتکل TCP/IP نیز ظاهر شده باشد.

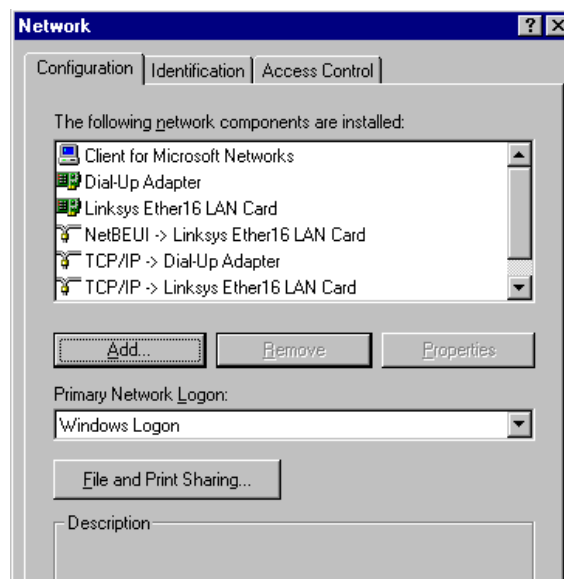
با حرکت نوار لغزنده روی TCP/IP → نام کارت شبکه را نیز خواهید دید یعنی اینکه کارت شبکه شما با پروتکل TCP/IP در ارتباط است طبق شکل (5-6).



شکل 5-6

4- برای اضافه کردن TCP/IP روی دکمه Add کلیک کنید.

5- روی گزینه Protocol دوبار کلیک کنید (شکل 6-6).

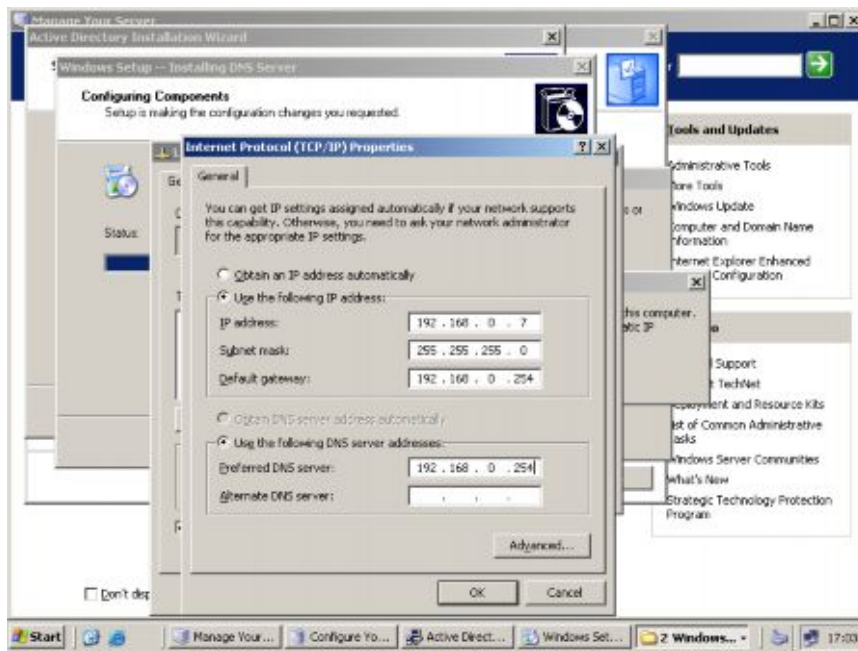


شکل 6-6

اگر پروتکل TCP/IP با کارت شبکه شما ارتباط نداشته باشد با دکمه Add پروتکل را می توان به کارت شبکه افزود.

6- برای Manu Features گزینه Microsoft را انتخاب کنید.

7- برای Network Protocol گزینه TCP/IP را انتخاب کنید (شکل 7-6)

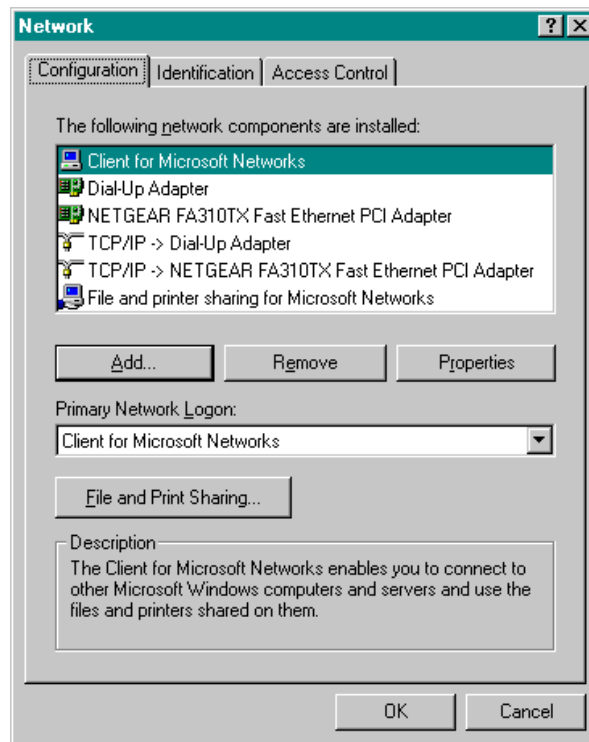


شکل 7-6

8- بعد از نصب آن از روی **CD-ROM** روی **OK** کلیک کنید تا کامپیوتر مجدداً راه اندازی شود. اکنون کامپیوتر شما روی شبکه قابل شناسایی است.

3-6- نامگذاری کامپیوتر و گروه کاری

- لازم است نامی را برای کامپیوترتان مشخص نمائید تا بوسیله آن در شبکه شناسایی شو (این قسمت با باز کردن گزینه **Network Neighborhood** در ویندوز 98 و یا باز کردن آیکون **Network Place** در **windows 2000/Me/XP** امکان پذیر است)
- برای این منظور مراحل زیر را طی می کنیم (شکل 8-6)
- 1- روی آیکون **Network Neighborhood** از **Desktop** راست کلیک نمائید.
 - 2- گزینه **Properties** را انتخاب کنید.
 - 3- روی دستگیره **Identification** کلیک کنید.



شکل 8-6

- 4- نامی را برای کامپیوتر انتخاب کنید سعی کنید نامی انتخاب کنید که در خاطرتان بماند.
- 5- نامی را برای گروه کاری انتخاب نمائید لازم بذکر است که تمام کامپیوترهای روی شبکه باید از نام گروه همانند استفاده نمایند.
- 6- در قسمت **Computer Description** توضیحی وارد نمائید.

7- روی دکمه **ok** کلیک کنید

بعد از انجام موارد فوق کامپیوتر شما روی شبکه قابل شناسایی است و می توان فایلهای و چاپگرها را به اشتراک گذاشت ویندوز این سرویس ها را ممکن است قبلاً ایجاد نماید ولی بهتر است آنها را نیز مجدداً چک نمائیم.

4-6- شروع اشتراک گذاری فایل ها و چاپگر

اشتراک گذاری فایل و چاپگر خیلی آسان است زمانیکه اشتراک گذاری را انجام دادید با مرور محتوای **Network Neighborhood** می توان کامپیوترهای شبکه را دید و فایل های اشتراک گذاری شده را دید و به خاطر داشته باشید که باید همیشه از یک **Eirewall** استفاده کنید تا شبکه شما را از دید کاربران غیر مجاز روی اینترنت مخفی نگه دارد. اگر شبکه شما مجهز به **Router** باشد ممکن است بصورت داخلی دارای **Firewall** نیز باشد. در صورت نبودن **Firewall** می توان بصورت رایگان یک نرم افزار **Firewall** از اینترنت **Download** نمود در این باره در فصل 11 بحث خواهد شد.

بعد از ذکر اخطار امنیتی نحوه اشتراک گذاری فایلهای و چاپگر را بیان می کنیم.

- 1- روی آیکون **Network Neighborhood** از **Desktop** راست کلیک نمائید.
- 2- گزینه **properties** را انتخاب کنید.
- 3- روی دکمه **File And Print Sharing** کلیک کنید.

5- گزینه "I want to be able to others to print to my printers" را انتخاب کنید

6- روی دکمه **ok** کلیک کنید

بعد از انجام مراحل فوق اکنون کامپیوتر شما آماده اشتراک گذاری است برای اشتراک گذاری فایل ها مراحل زیر را انجام می دهیم

1- دایرکتوری را که می خواهید اشتراک سازی کنید فعال نمائید.

2- روی آن راست کلیک کرده و گزینه **Sharing** را انتخاب نمائید.

3- از پنجره باز شده گزینه "**shared As**" را انتخاب کنید.

4- نحوه اشتراک گذاری آن ر برای کاربران تعیین نمائید یعنی حالت **Read only** برای فقط خواندن و **Full** برای خواندن و تغییر دادن.

5- اگر شما حالت **Full** یا **Deoends on Password** را انتخاب نمائید لازم است کلمه رمزی را نیز تعیین کنید.

6- در صورت انتخاب حالت **Full** یا **Depend on Password** یک کلمه رمز به جعبه متن اختصاص دهید.

7- روی دکمه **ok** کلیک کنید.

بعد از انجام مراحل فوق اکنون پوشه شما اشتراکی شد.

حال نوبت آن رسیده که نحوه اشتراک گذاری چاپگر را برایتان شرح دهیم:

1- روی **My Computer** دوبار کلیک کنید.

2- روی گزینه **Printers** دوبار کلیک کنید.

3- روی آیکون چاپگری که می خواهید به اشتراک گذارید راست کلیک نمائید.

4- گزینه "**sharing**" را انتخاب کنید.

5- اگر آن را قبلاً انتخاب نکرده اید گزینه **Shared as** را انتخاب نمائید.

6- روی دکمه **ok** کلیک کنید.

حال چاپگر شما بصورت اشتراکی در شبکه قابل استفاده است.

در بخش بعدی نحوه استفاده از پوشه ها و چاپگرهای اشتراکی گذاری شده را توسط آیکون **Network Neighborhood** از **Desktop** شرح خواهیم داد.

6-5- استفاده از شبکه مجاور یا Network Neighborhood

برای یافتن منابع اشتراکی شده لازم است از **Desktop** آیکون **Network Neighborhood** را باز کنیم با باز شدن آن تمام کامپیوترهای موجود در روی شبکه ظاهر خواهند شد. (شکل 6-9)



شکل 6-9

همچنین برای مشاهده منابع اشتراکی می توان روی آیکون **Network Neighborhood** راست کلیک نموده و گزینه **Properties** را انتخاب کرد این کار باعث خواهد شد که بتوانید تنظیمات شبکه را که کامپیوتر شما از آن استفاده می کند را مشاهده نمائید.

با استفاده از جعبه گفتگوی **Properties** آیکون **Network Neighborhood** می توان اشتراکی بودن فایل و چاپگر را فعال و یا غیر فعال نمود و یا اینکه تنظیمات کارت شبکه را تغییر داد از قبیل پروتکل ارتباطی **TCP/IP** که قبلاً در ابتدای فصل درباره آن بحث شد.

با استفاده از **dialog Box** مربوط به **properties** میتوان نام کامپیوتر و نام گروه کاری را تغییر داد این عمل با انتخاب گزینه **Identification** موجود در **properties** امکان پذیر است.

6-6- دسترسی اشتراکی به اینترنت بصورت بی سیم

اگر شما کامپیوتری را بصورت دسترسی به اینترنت طراحی نموده اید می توانید با نرم افزار اشتراک گذاری اتصال به اینترنت یا (**Internet Connection Sharing Software**) آن را به کامپیوترهای شبکه نیز تعمیم داد یعنی کافی است با اتصال این کامپیوتر به اینترنت و اشتراکی کردن دسترسی به اینترنت سایر کامپیوترهای موجود در شبکه نیز اینترنت استفاده نمایند. لازم به یاد آورید بهتر است برای این کار از یک **Router** که امکان اشتراک سازی اتصال به اینترنت را داشته باشد استفاده نمایید. در فصل 9 در این باره مفصلاً بحث خواهیم نمود.

اگر شما از **ICS** به جای یک **Router** استفاده کنید لازم است یک کامپیوتر همیشه به اینترنت متصل شود تا سایر کامپیوترها در صورت دلخواه از اینترنت استفاده نمایند.

استفاده از **Router** جهت اشتراکی کردن اینترنت بعلاوه از سایر مزایا دارای این مزیت نیز هست که شبکه کامپیوتری شما را از دید هکرها مخفی کرده و در برابر آنها محافظت می نماید.

اگر سیستم عامل موجود در کامپیوتر شما ویندوز **XP** یا **2000** است می توانید در فصل بعد نحوه اتصال کامپیوتر به شبکه را مشاهده نمایید و اگر شما **Router** نیز دارید نحوه اتصال اشتراکی به اینترنت را در فصل 8 خواهید دید.

6-7-خلاصه فصل

زمانیکه سخت افزار کارت شبکه به کامپیوتر شما وصل گردید فقط لازم است از تشخیص و شناسایی کارت شبکه بی سیم توسط سیستم عامل مطمئن شوید بعد از آن سیستم عامل ویندوز تمام نرم افزارهای مورد نیاز شما جهت اتصال کامپیوترها به یکدیگر و اشتراک داده ها را مبرای می کند.

ممکن است در اذهان چنین تداعی شود که شبکه کامپیوتری بی سیم در ابتدای کار ممکن است کمی ترسناک باشد در حالیکه چنین نبوده و به مراتب از سایر شبکه های آسان است برای اشتراکی کردن فایلها و چاپگرها لازم است پروتکل **TCP/IP** روی کامپیوترها نصب شوند برای فایل ها و چاپگرها نیز خاصیت اشتراکی تعریف شده و فعال شوند.

7- آموزش گام به گام شبکه سازی در ویندوز XP

در این فصل داریم

1-7- اطمینان از شناسائی سخت افزارها

2-7- نصب و بروزرسانی درایوها

3-7- تغییر تنظیمات دستی

4-7- اشتراک سازی فایل و چاپگر

5-7- اشتراک سازی دسترسی به اینترنت

6-7- استفاده از جادوگر نصب شبکه یا **Network Setup Wizard**

7-7- خلاصه فصل

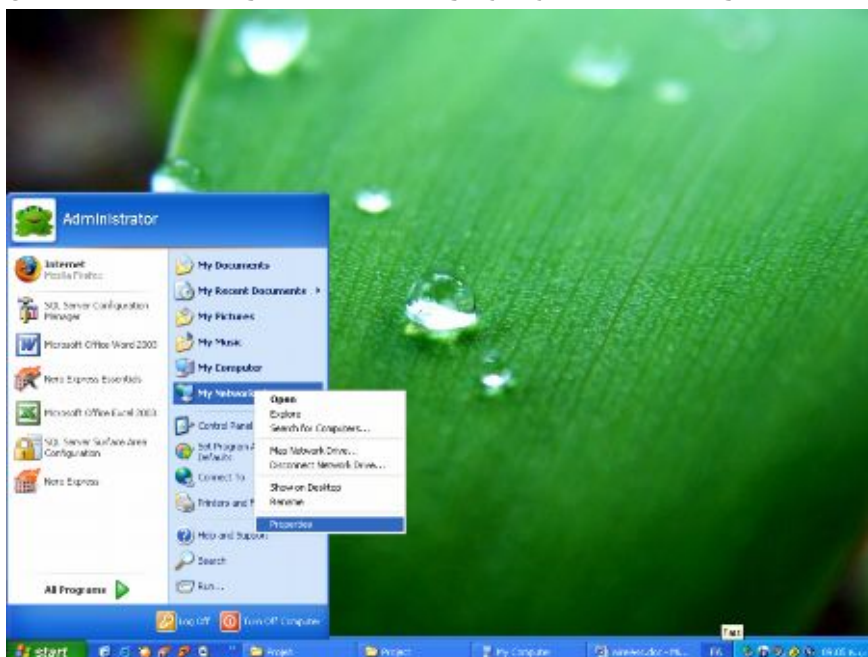
اگر از ویندوز XP استفاده می کنید شما شانس خوبی دارید این سیستم عامل دارای خصوصیات اشتراکی کردن فایلها و اینترنت در شبکه را به نحو احسن ارائه می کند استفاده از درایورهای بروز کارت شبکه بی سیم در ویندوز XP خیلی مهم است زیرا اگر از درایورهای جدید استفاده نکنید با مشکلات زیادی روبرو خواهید شد.

ما در این فصل برای نصب و راه اندازی شبکه به دو دلیل از ویندوز XP استفاده کرده ایم اول اینکه ویندوز XP آخرین و جدیدترین سیستم عامل شرکت ماکروسافت می باشد و در آن امکانات کامپیوترهای جدید گنجانیده شده دوم اینکه از این طریق کاربران ویندوز 2000 نیز قادر به اجرا و بکارگیری آن هستند زیرا تقریباً امکانات ویندوز XP شبیه ویندوز 2000 است برخلاف ویندوز 2000 در ویندوز XP استفاده از **Network setup wizard** کمکی ساده تر است هر چند استفاده از **wizard** مانند سایر چیزها باعث سادگی عملیات می شود. در حقیقت گاهی اوقات استفاده از امکانات ساده باعث بروز اشتباه می شود پس بهتر است با نحوه بکارگیری تنظیمات دستی شبکه و نحوه تغییر این تنظیمات آشنا شوید.

7-1- اطمینان از شناسایی سخت افزار

اولین قدم در شبکه سازی ویندوز XP اطمینان یافت از شناسایی کارت شبکه توسط سیستم عامل است فهمیدن این موضوع آسان است ابتدا لازم است از نظر سخت افزاری مطمئن شویم که کارت شبکه شما در پورت **PCI** (برای کامپیوترهای رومیزی) یا پورت **USB** (برای **laptop**ها و **Desktop**ها) یا شیار **pc** کارت (برای **laptop**ها) به صورت صحیح و کامل جا افتاده است. اگر از اتصال صحیح آن مطمئن شوید در پشت این کارت عموماً چراغ به رنگ سبز خواهید دید حال می خواهید از شناسایی کارت شبکه توسط سیستم عامل ویندوز XP مطمئن شویم.

1- روی **My Computer** راست کلیک نموده و گزینه **properties** را انتخاب کنید (شکل 7-1)



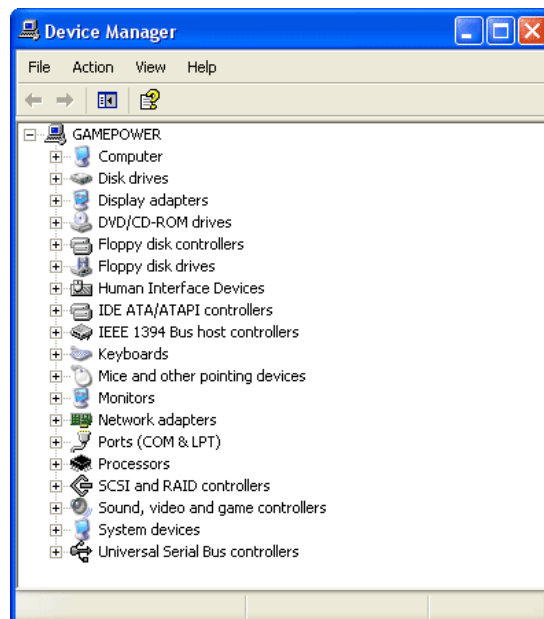
شکل 7-1

2- روی دستگیره **hardware** کلیک کرده سپس دکمه **Device manager** را انتخاب نمایید. (شکل 7-2)



شکل 2-7

3- در لیست دستگاه ها روی علامت + گزینه **Network Adaptor** کلیک نمائید. (شکل 3-7)



شکل 3-7

در صورت شناخته شدن در ویندوز باید نام کارت شبکه شما نیز موجود باشد در صورت نبودن نام کارت شبکه لازم است آنرا از CD مربوطه مجدداً نصب نمائید.

2-7- نصب و بروز رسانى درايورها

اگر کارت شبكه شما بعد از نصب نيز كار نكرد اين صورت ممكن است درايور نصب كارت شبكه نياز به **Update** داشته باشد كه در اين حالت لازم است به سايت كارخانه سازنده آن متصل شده و آخرين نسخه نرم افزار كارت شبكه را **Download** نماييد.

در زير نام تعدادى از سازندگان كارت شبكه به همراه سايت مربوطه ارائه شده است كه مى توان با اتصال به آن سايت ها آخرين نسخه **Driver** كارت شبكه را **Download** نمود.

3com (support.3com.com)

Copaq(www.compaq.com/support/files/Networking/)

D-link(www.dlink.com/tech/)

LinkSys(www.lunicsys.com/download/)

Proxim(www.proxim.com/support/software/)

Net gear (4-7 شكل) (support1.Netgear.com/netgear1/)

SMC(www.SMC.com)

Intel(Support.intel.com)



شكل 4-7

استفاده از اين درايورهاى بروز باعث خواهد شد كه كارت شبكه شما توسط سيستم عامل قابل شناسايى شده و امكان ارتباط بوجود آيد. همچنين استفاده صحيح از درايور كارت شبكه باعث بالا رفتن سرعت و توان عملياتى شبكه خواهد شد.

7-3- تغییر تنظیمات دستی

چنانچه قبلاً ذکر کردیم ویندوز XP را روی گزینه **Networking wizard** می باشد که می تواند به تنظیمات تمام کامپیوترهای موجود در شبکه کمک کند اگر شما استفاده از **wizard** را ترجیح می دهید. می توان به صورت سریع تنظیمات دستی را انجام داد برای این منظور می توانید به قسمت « استفاده از **Network setup wizard** » مراجعه نمائید که در این فصل می باشد.

ابتدا می خواهید از وجود نام برای کامپیوتر اطمینان حاصل نمائید پس لازم مراحل زیر را طی نمائید.

1- از **start Menu** (یا از **desktop** در صورت وجود **My Computer**) روی **My Computer** راست کلیک نموده سپس گزینه **properties** را انتخاب کنید.

2- روی دستگیره **Computer Name** کلیک کنید.

3- در قسمت **Computer Description** توضیحی را برای کامپیوتر وارد نمائید.

4- اگر می خواهید نام کامپیوتر را تغییر دهید روی دکمه **Change** کلیک کنید.

5- پنجره تغییر نام کامپیوتر **Computer Name Change** باز می شود.

در جعبه محاوره ایجاد شده نام کامپیوترتان را وارد کنید همچنین می توان نام گروه کاری را نیز ایجاد نمود لازم بذکر است که باید گروه کاری تمام کامپیوترها یکی باشد.

6- در صورت نبودن نام برای گروه کاری در قسمت **Workgroup** نام گروه کاری را وارد کنید.

توجه:

می توان از نامهای متفاوت برای گروه های کاری استفاده نمود این کار موقعی صورت می گیرد که شما از چندین شبکه متفاوت محلی استفاده می کنید هر چند کار باعث خواهد شد که شما گروه های کاری جداگانه داشته باشید که از طریق **My Network Place** می توان مشاهده نمود زمانیکه شما برای کامپیوتر و گروه کاری نامگذاری نمودید می توانید واقعا وارد مرحله شروع به کار شبکه شوید و چاپگرها و فایلها را اشتراکی نمائید.

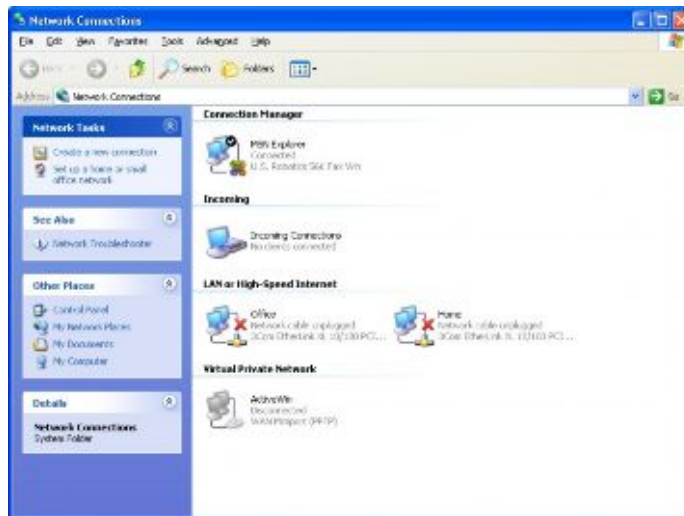
4-7- اشتراک سازی فایل ها و چاپگر

سرویس های اشتراکی سازی فایل ها و چاپگر در ویندوز XP بصورت پیش فرض فعال هستند این بدین مفهوم است که موقع نصب مناسب کارت شبکه بی سیم روی کامپیوتر باید قادر به اشتراکی کردن فایل ها و چاپگرها باشید. برای اطمینان از اشتراکی شدن فایل ها و چاپگرها و فعال بودن آنها مراحل زیر را باید طی نمود:

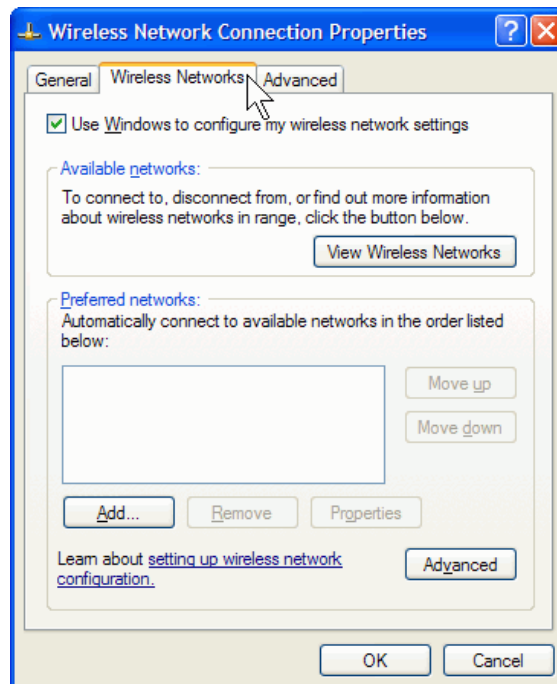
1- start menu (یا از Desktop روی My Network Place راست کلیک کرده و گزینه properties را انتخاب کنید (شکل 5-7).

2- روی نام کارت شبکه بی سیم راست کلیک کرده و گزینه properties را انتخاب نمائید (شکل 6-7).

3- گزینه File and printer sharing for Microsoft Network را خواهید دید.



شکل 5-7



شکل 6-7

3- اگر جعبه چک گزینه **File and printer sharing** علامتگذاری نشده باشد به آن علامت چک بزیند سپس روی دکمه **ok** را زده و جعبه محاوره باز شده بسته خواهد شد.

آیکون **My computer Place** مانند یک پوشه کار می کند که در آن منابع شبکه قرار داده شده است می توان با استفاده از آن کامپیوترها و چاپگرهای اشتراکی شده را دید و یا خصوصیات کارت شبکه بی سیم را مرور نمود.

بعد از یادگیری اشتراکی کردن فایلها و چاپگرها اجازه دهید با نحوه اشتراک گذاری دسترسی به اینترنت در ویندوز **XP** را شرح دهیم.

7-5- اشتراکی کردن دسترسی به اینترنت

می توان دسترسی به اینترنت از طریق مودم **dial up (56kbps)** یا مودم کابلی یا **DSL** را اشتراکی نمود ساده ترین روش برای این کار استفاده از **Network setup wizard** می باشد. اگر از یک **Router** استفاده می کنید مطالب بیشتری را در فصل 8 مشاهده کنید اما اگر می خواهید فقط یک کامپیوتر به اینترنت وصل شده و سایر کامپیوترها از طریق شبکه ایجاد شده بوسیله ویندوز **XP** به اینترنت وصل شوند لازم است مراحل زیر را مرحله به مرحله طی نمائید.

1- آیکون **My Network Place** را باز کنید.

2- از پنجره باز شده در قسمت **Network Task** روی گزینه "**view network connection**" کلیک نمائید.

4- روی گزینه **wireless connection** راست کلیک کرده و گزینه **properties** را انتخاب نمائید.

4- روی دستگیره **Advanced** (پیشرفته) کلیک کنید.

5- گزینه "**Allow other network user to connect through this computers internet connection**" را انتخاب نمائید (شکل 7-7).



شکل 7-7

6- گزینه **connection** را از زیر شاخه "**Home Networking connection**" برای اشتراکی کردن انتخاب کنید.

7- روی دکمه **ok** کلیک نمائید.

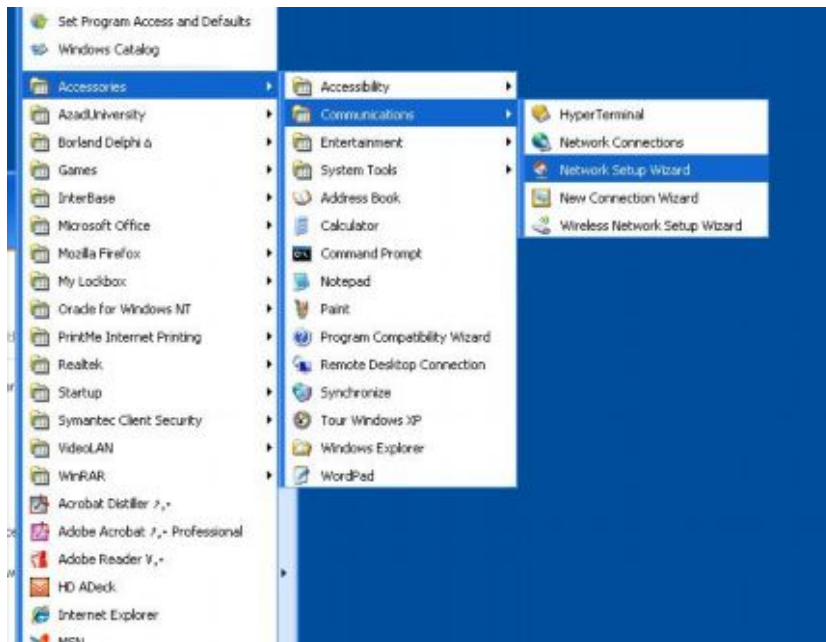
اکنون کامپیوتر شما به عنوان یک **Router** روی شبکه انجام وظیفه می کند بیاد داشته باشید سایر کامپیوترها موقعی به اینترنت وصل می شوند که کامپیوتر شما به اینترنت متصل شده باشد.

7-6- استفاده از جادوگر نصب شبکه یا **Network setup wizard**

اگر می خواهید شبکه کامپیوترتان را بصورت دستی تنظیم و راه اندازی نمائید می توانید از گزینه **Network setup wizard** مربوط به سیستم عامل ویندوز **XP** استفاده کنید با امکانات و اسباب هایی که ویندوز **XP** در اختیارتان می گذارد در چند دقیقه تمام مراحل راه اندازی شبکه را طی نمائید مراحل استفاده از **wizard** نصب شبکه به صورت زیر است.

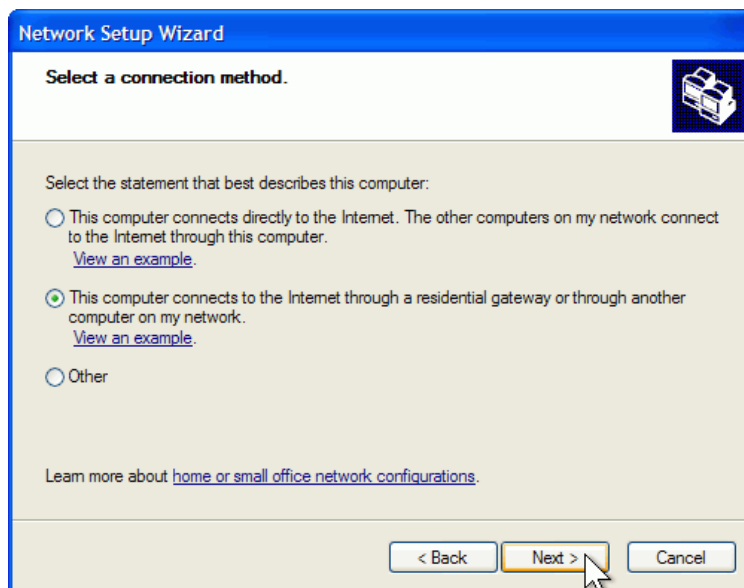
1- گزینه **My Network Place** را از **Desktop** یا **start menu** باز کرده و در قسمت **Network Tasks** گزینه " **setup a home or small office Network**" را انتخاب کنید این قسمت را با استفاده از طی مراحل

start → **All programs** → **Accessories** → **communication** → **Network setup wizard** می توان انجام داد (شکل 7-8).



شکل 8-7

2- پنجره **Network setup wizard** باز می شود اگر بخواهید ارتباط دسترسی به اینترنت نیز اشتراکی شود گزینه "**This computer connect directly to the Internet**" را طبق شکل 9-7 انتخاب کنید.



شکل 9-7

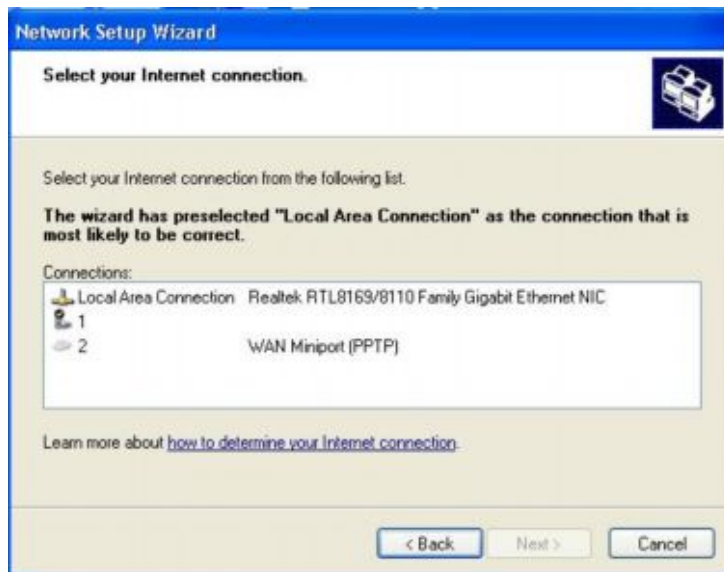
اگر شما از یک **Router** استفاده می کنید لازم است روی گزینه دوم یعنی

"This computer connects to the Internet through another computer on my network or residential gateway"

کلیک نمائید.

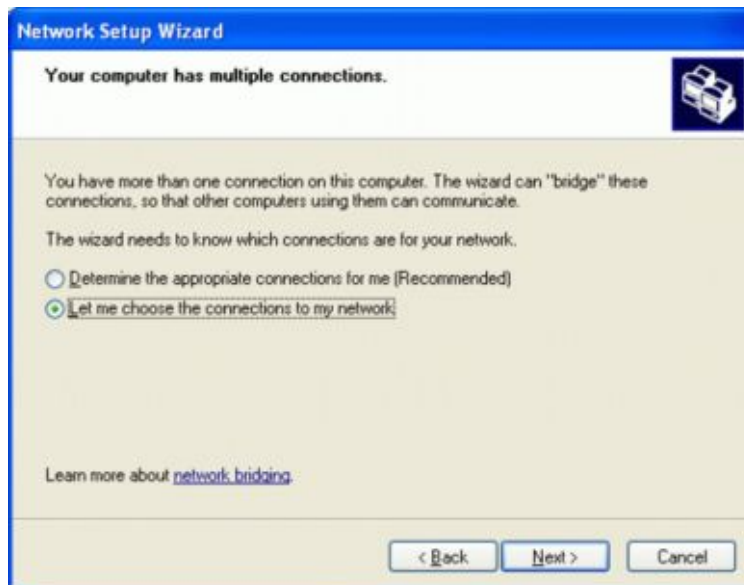
3- اتصال اینترنتی **Internet Connection** که می خواهید بصورت اشتراکی درآید را انتخاب نمائید. شکل (7-10) در این نمونه من یک **dial up modem** برای اتصال به **ISP** خودم را اشتراکی نموده ام بخاطر داشته باشید ممکن است اتصال به اینترنت شما بصورت اتصال بی سیم نباشد و استفاده از اینترنت بصورت سیمی از قبیل مودم انجام گیرد.

استفاده از اتصال بی سیم بصورت اشتراکی در گام های بعدی بحث خواهد شد. روی دکمه **Next** کلیک کنید.



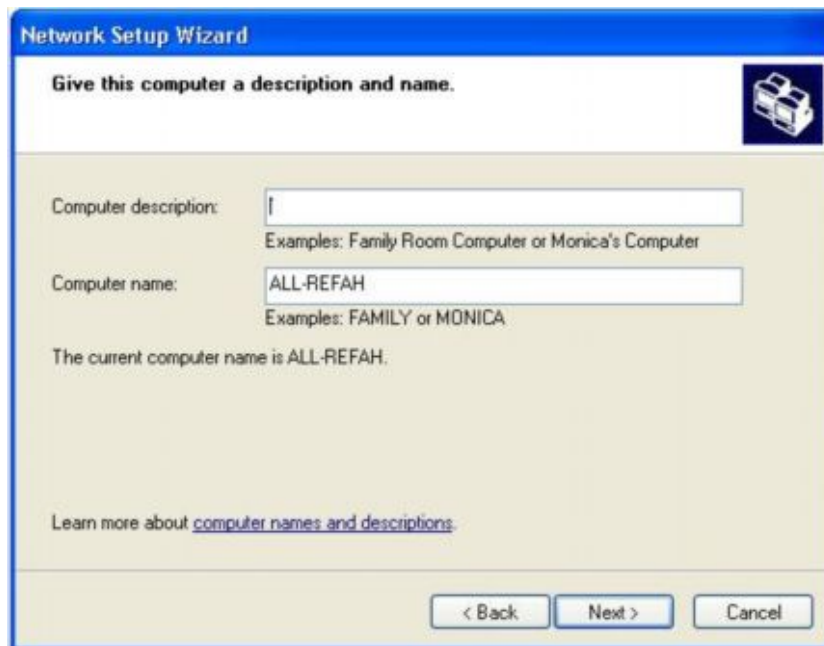
شکل 7-10

4- استفاده از **wizard** می تواند اتصال شبکه را بصورت اشتراکی تعیین کند (شکل 7-11) این عمل بهتر است اگر بخواهید اتصال را بصورت اشتراکی استفاده نمایید لازم است گزینه **" Let Me choose the connections to my Network"** را انتخاب نمایید.



شکل 7-11

5- برای کامپیوترتان نامی را انتخاب کنید (باید نام کامپیوترتان منحصر بفرد باشد) توضیحاتی را در قسمت **Computer description** که چند کلمه می باشد وارد نمایید (شکل 7-12) روی دکمه **Next** کلیک کرده و یک نامی را برای گروه کاری تعیین کنید نام گروه کاری به صورت پیش فرض **MSHOME** می باشد. که می توانید به صورت دلخواه آن را عوض نمایید باید توجه داشته باشید که نام گروه کاری برای تمام کامپیوترها باید یکسان باشد روی دکمه **Next** کلیک نمایید.



شکل 7-12

6- استفاده از **wizard** تمام انتخاب ها ممکن را نشان می دهد و شما را از تمام چیزهایی که می خواستید مطمئن می سازد اگر در آن مشکلی مشاهده نمودید می توانید با استفاده از دکمه **Back** به مراحل قبلی برگشته و تنظیمات را تعویض نمائید ولی اگر تمام چیزهای نشان داده شده طبق انتخاب شما بود می توانید روی دکمه **Next** کلیک نموده تا شبکه شما آماده کار باشد.

زمانیکه مراحل نصب **wizard** پایان یافت با درست کردن یک دیسک راه اندازی شبکه برای سایر کامپیوترها عملیات شبکه سازی را خیلی سریع می نماید بجای ایجاد دیسک های جداگانه می توان از **CD** ویندوز **XP** استفاده نمود برای این منظور **CD** مربوطه را در درایو قرار داده و توسط ویندوز **98** یا **Me** گزینه **"perform additional Task"** را انتخاب کنید. بعد از آن گزینه **Setup a home or small office network** را انتخاب کنید. با استفاده از دیسک نصب **XP** می توانید سایر کامپیوترهای موجود در شبکه را بطور اتوماتیک نصب نمائید.

اگر در مراحل نصب شبکه بصورت دستی یا **wizard** با مشکلاتی مواجه شدید لازم است به فصل **10** مراجعه نمائید.

7-7- خلاصه فصل

نصب شبکه بی سیم در ویندوز XP با شناسایی کلیه قطعات سخت افزاری شروع می شود و می توانید آخرین نسخه درایورهای مورد نیاز را نصب نمائید لازم است برای ایجاد شبکه نامی را برای کامپیوترتان مشخص نمائید ممکن است ویندوز XP را به طور پیش فرض نامی را برای کامپیوترتان تعیین کرده باشد. این عمل را برای گروه کاری **workgroup** یا نیز باید انجام داد لازم به یادآور است که نام گروه کاری باید بر روی کلیه کامپیوترهای موجود در شبکه یکسان باشد ویندوز XP بطور پیش فرض خاصیت اشتراک سازی فایل ها و چاپگرها را فعال می کند. ولی بهتر است قبل از استفاده از آن صحت اشتراک سازی آنها را چک نمائیم اگر بخواهید وظایف فوق را بصورت دستی انجام دهید. بسادگی توسط **Home Network Wizard** با طی مراحل **wizard** امکان پذیر است.

8- روترها و اشتراک سازی اینترنت

در این فصل داریم

1-8- انتخاب کردن یک روتر بی سیم

2-8- اضافه نمودن **Router** به شبکه

3-8- نصب **ICS windows (windows Internet connection shared)** روی کامپیوتر میزبان

4-8- تنظیم کامپیوترهای موجود در ایستگاه های کاری

5-8- خلاصه فصل

اکنون چگونگی ایجاد و راه اندازی یک شبکه کوچک محلی را یاد گرفته اید اجازه دهید کمی بیشتر درباره امکان اتصال شبکه به اینترنت بحث نمائیم خصوصاً درباره نحوه کار **Router** , **Gateway** و نحوه ایجاد شبکه سالم توسط آنها صحبت خواهیم کرد.

در کل استفاده از **Router** جهت اتصال شبکه به اینترنت دارای دو مزیت زیر است

1- وجود یک **Router** در شبکه باعث می شود شبکه شما در برابر افرادی که توسط ترجمه آدرس شبکه یا **NAT (Network address Translation)** متصل می شوند محافظت شده و فقط یک آدرس **IP** برای کل شبکه هنگام اتصال به اینترنت نمایش داده می شود یعنی کلیه کامپیوترهای شبکه محلی فقط توسط یک آدرس **IP** بر روی اینترنت شناسایی می شوند.

2- روتر با **DHCP (Dynamic Host configuration protocol)** تخصیص آدرس **IP** برای کامپیوترهای موجود در شبکه بصورت دستی را امکان پذیر می سازد بطوریکه در اینترنت آدرس های بزرگ و زیادی نمایش داده نمی شوند.

کل امکانات **Router** در بالا بیان نشده است **Router** ها **NAT** و **DHCP** را تهیه می کند آیا می توانید از **Router** استفاده نمائید احتمالاً بتوانید اجازه دهید توسعه هایی را برای انتخاب **Router** سیمی و بی سیمی برایتان گوشزد نمائیم.

8-1- انتخاب کردن یک روتر بی سیم

اگر می خواهید شبکه خانگی طراحی کنید که چندین ماشین بصورت اشتراکی به اینترنت وصل شوند استفاده و بکارگیری یک **Router** بی سیم آسان و مفیدتر است برای استفاده بهتر از این **Router** خرید **Router** که در آن **Access Point** بی سیم نیز تعبیه شده باشد توصیه می گردد.

خرید **Router** به همراه **Access Point** به شما امکان خواهد داد که بتوانید بیش از یک ارتباط ایجاد نمائید بعضی از **Access Point** ها دارای خصوصیات مفید دیگری از قبیل **hub printer server** یا مودم ارتباطی آنالوگ برای پشتیبانی پهن باند ارتباط نیز می باشند.

با پائین آمدن قیمت **Access Point** با **Router** باعث شده شرکت های سازنده خصوصیات ذکر شده را جهت ماندن در بازار رقابت اضافه می کنند.

در بخش بعد درباره خرید یک **Router** جدا برای شبکه های بی سیم بحث خواهیم کرد فرض می کنیم شما قبلاً یک شبکه سیمی دارید در این حالت می توان با استفاده از یک **Access Point** بی سیم به یک **Router** سیمی متصل گردید در این شبکه اگر شما دارای **setup** متفاوتی در دو طرف باشید (منظور اینکه ارتباط بین دو شبکه اساساً از طریق اتصال یک **Access Point** و یک **Router** سیمی است) تفاوتی بین کار **Router** با **Access Point** داخلی وجود ندارد. پیکربندی یک **Router** سیمی شبیه پیکربندی **Router** بی سیم می باشد. در بخش آخر این فصل نحوه راه اندازی **Router** بیان شده است.

موضوعی که در این جا احتمالاً بیان شود این است که در یک محیط کوچک مثل خانه یک **Router** سیمی ممکن است دارای تکنولوژی جدید **No- new-wires** نباشد و نیاز به سخت افزاری از قبیل خط تلفن یا خطوط نیرو باشد تجهیزات شبکه سازی خطوط تلفن ارزان قیمت و تجهیزات شبکه خطوط نیرو با فرصت

های شبکه سازی فراوان می باشد بنابراین استفاده از هر دو تکنولوژی ذکر شده بصورت یکجا و همزمان خیلی مفیدتر بنظر می رسد.

از آنجائیکه تجهیزات خطوط تلفن ممکن است از نظر بودجه مقرون به صرفه باشد می توانید از یک پل خط تلفن به اترنت به هاب وصل شوید **phone line – to- Ethernet** و توسط این هاب که به **Access Point** متصل شده به تمام کارتهای شبکه بی سیم وصل شد. با ترکیب دو تکنولوژی باعث صرفه جویی در هزینه ها خواهید شد استفاده از کارتهای شبکه خط تلفن بمراتب ارزانتر از کارتهای شبکه بی سیم بوده و دارای سرعت یکسانی هستند در اینجا راههای ممکن استفاده از یک **Router** سیمی در شبکه بی سیم بیان شده است.

1- اتصال **Router** به یک **hub** متصل به شبکه **Ethernet** اتصال **Access Point** به **hub**

2- اتصال خط تلفن یا پل خط نیرو به یک **hub** اتصال **Access Point** به **hub** اگر شما قبلاً **Router** سیمی داشته باشید دیگر نیاز به صرف هزینه اضافی جهت خرید **Router** بی سیم نیست و فقط خرید **Access Point** کافی است فقط به خاطر داشته باشید که این سخت افزار سیمی می تواند باعث توسعه شبکه و امکان ایجاد شبکه با چند تکنولوژی شود.

8-2- اضافه نمودن **Router** به شبکه

برای اضافه کردن **Router** به شبکه زمان زیادی لازم نیست فقط کافی است که یک پورت **Router** را به بودن پهن باند و پورت دیگر را به **Access Point** وصل کنید. در بعضی وقت ها ممکن است **Router** جهت کار باشبکه تنظیم نشده باشد **Router** های جدید که به بازار آمده اند طوری طراحی شده اند که به طور اتوماتیک هنگام خرید ایجاد ارتباط به شبکه تنظیم می شوند که اصطلاحاً **user friendly** گوئیم. اگر **Router** شما نیاز به تنظیمات دستی باشد چندین روش برای اطمینان از ایجاد **IP** آدرس برای کامپیوترهای شبکه و ایجاد ارتباط با اینترنت وجود دارد.

فهمیدن این موضوع **ISP** مورد استفاده برای ایجاد آدرس **IP** بصورت استاتیک عمل می کند یا دینامیکی مهم است در حالت استاتیک **ISP** فقط یک **IP** آدرس تولید می کند و آن تغییر نمی کند اکثر **ISP** ها بصورت دینامیکی عمل می کنند و **IP** آدرس بنا به صلاحدید **ISP** تغییر می کند مودمهای **Dial – up** نوعاً در هر ارتباط آدرس **IP** جدیدی به کاربران ارائه می کنند مودم های **DSL** یا کابلی نیز مکن است در هر روز آدرس **IP** جدیدی به کاربران ارائه نماید.

اگر **ISP** آدرس **IP** استاتیک تولید می کند به سادگی می توانید با وارد کردن این آدرس **Router,IP** را راه اندازی نمائید اکثراً می توان به **Router** ها با باز کردن مرورگر **Web** و وارد کردن آدرس **IP** (نوعاً **192.168.0.1** یا **192.168.1.1**) دسترس داشت .

آدرس های **192.168.0.1** تا **192.168.0.254** به عنوان آدرس های زیر شبکه یا **subNet** بکار می روند و فقط در داخل شبکه قابل شناسایی بوده و در اینترنت دیده نمی شوند.

می توان آدرس های **IP** را از طریق **ISP** ایجاد نمود یا اینکه بصورت دینامیکی هنگام وصل شدن به **ISP** ایجاد شود این روش بنظر آسان می رسد اما گاهی اوقات بعضی از **Router** ها با تنظیمات دستی خاص نیاز به آشنایی کامل به نحوه تنظیم و نحوه دسترسی به **Router** دارند.

گاهی لازم است سایر تنظیمات را نیز تغییر دهیم اما آنها شبیه حالت پیش فرض هستند این تنظیمات عبارتست از تنظیم و راه اندازی سرویس دهنده نام حوزه یا DNS (Domain Name Server) است منظور از DNS ترجمه نام حوزه اینترنت (مانند .com یا .edu و ..) یک آدرس IP منحصر بفرد است که توسط آن یک کامپیوتر روی اینترنت تشخیص داده می شود. برای مثال یک وب سایت دارای یک آدرس IP منحصر بفرد است که این آدرس به نام حوزه وابسته نشده است DNS این آدرسها را ترجمه می کند اکثر ISPها داده را بطور مستقیم از این DNS به Router عبور می دهند و نیاز به وارد کردن آنها ندارند. اما اگر نیاز به وارد کردن آن باشد. فقط با نوشتن آدرس IP در سرور سریعاً ISP آن را تهیه خواهد نمود.

8-3-3- نصب windows ICS (windows Internet connection sharing) روی کامپیوتر میزبان

اشتراک سازی ارتباط اینترنتی یا (Internet connection sharing) یکی از امکانات ویندوز است که در نسخه های window 98 SE و نسخه های بعد از آن بوجود آمده است. در فصل 7 بیان کردیم که window XP بوسیله Home Networking Wizard اشتراک سازی ارتباط اینترنتی را ایجاد می کند. می توان با مرور مراحل نصب آن برای Window ME که از ICS شبیه 98SE استفاده می کند استفاده نمود. Windows ME نیز برای دارای Home Networking wizard می باشد که می تواند بطور اتوماتیک فرآیند اشتراک سازی اینترنت را انجام دهد. بنابراین در اینجا نحوه نصب ICS به طور دستی را بیان می کنیم. برای شروع کار استفاده از یک Router روشی ساده و مفید برای دسترسی اشتراکی به اینترنت می باشد در این حالت چون می خواهیم مراحل ICS را بصورت دستی انجام دهید پس نباید توسط سیستم عامل نصب گردد. در اینجا استفاده از خصوصیات ICS را windows 98 SE یا window 98 ME شرح می دهیم. مهمترین قسمت کار این است که مطمئن شوید قبلاً برنامه ICS نصب نگردیده باشد بنابراین برای نصب لازم است CD ویندوز را در CD درایو قرار دهید.

8-3-1- مراحل نصب ICS

- 1- از start و از گزینه setting گزینه control panel را انتخاب کنید.
- 2- روی گزینه Add/ Remove Program دوبار کلیک کنید (شکل 8-1).



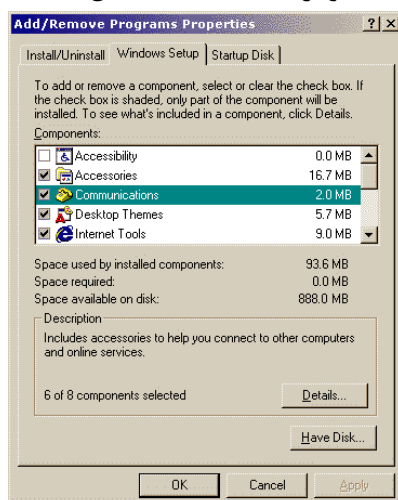
شکل 8-1

3- از پنجره ظاهر شده دستگیر **windows setup** را انتخاب کنید (شکل 8-2).



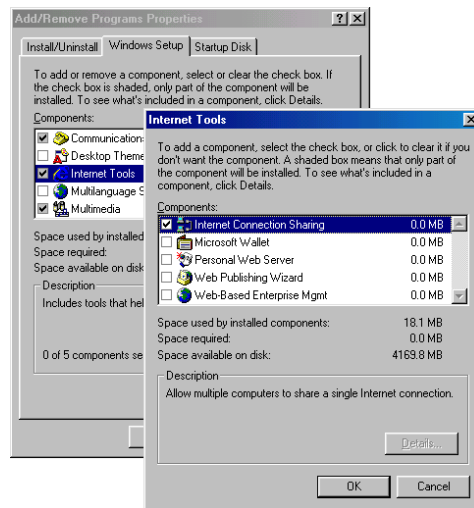
شکل 8-2

4- در **windows 98 SE** روی گزینه **Internet Tools** دوبار کلیک نمائید. (اگر از **windows ME** استفاده می کنید روی گزینه **communication** دوبار کلیک کنید) (شکل 8-3)



شکل 8-3

6- گزینه **Internet connection shareing** را انتخاب کرده و روی دکمه **ok** کلیک کنید (شکل 8-4)



شكل 4-8

در window 98 SE برنامه **Internet connection shareing** در ويندوز ME برنامه **Home Networking wizard** شروع بكار خواهد كرد . بعد از طى مراحل ذكر شده خصوصيات **Internet connection shareing** آماده اجرا است.

بعد از پايان مرحله **wizard ICS**, روى سيستم نصب شده و مى توان با استفاده از گزینه **Internet Option** موجود در **control panel** خصوصيات **ICS** را فعال و يا غير فعال نمود براى اين منظور مراحل زير را طى مى كنيم.

1- از **start** , **setting** گزینه **control Panel** را انتخاب كنيد.

2- گزینه **internet option** را انتخاب كنيد (شكل 5-8)



شكل 5-8

3- دستگيره **connections** را انتخاب كنيد(شكل 6-8).



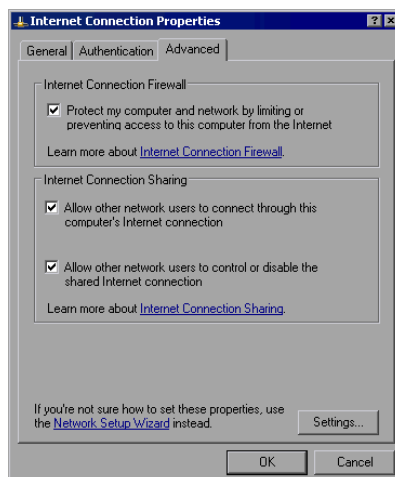
شکل 6-8

4- در تنظیمات Local Area Network (LAN) روی دکمه sharing کلیک کنید (شکل 7-8).



شکل 7-8

5- در پنجره باز شده توسط sharing با انتخاب گزینه Enable Internet connection sharing خصوصیات ICS فعال و در صورت حذف حالت انتخاب خصوصیات ICS غیر فعال می شود (شکل 8-8).



شکل 8-8

توجه داشته باشید که با استفاده از **Internet Explorer** می توان به منوی مشابهی دسترسی پیدا کرد برای این کار از منوی **Tools** گزینه **Internet option** را انتخاب می کنیم که همان منوی مرحله سوم می باشد. اکنون یکی از کامپیوترهایتان دارای خصوصیت اشتراک ارتباطی است در بخش بعد نحوه بکارگیری از این خصوصیت برای سایر کامپیوترها را بیان می کنیم.

8-4- تنظیم کامپیوترهای موجود در ایستگاههای کاری

در جریان استفاده از **Internet connection sharing wizard** در **windows 98SE** (در **windows ME** هنگام استفاده از **Home Network wizard**) دیسک راه اندازی شبکه ایجاد می شود که با استفاده از این دیسک سایر کامپیوترها نیز به سادگی می توانند راه اندازی شده و به شبکه متصل شوند مهمترین مسئله ای که باید یادآور شویم این است که مطمئن شویم که تمام کارتهای شبکه بی سیم دارای پروتکل **TCP/IP** هستند.

در فصل بعد نحوه تنظیم مرورگر روی کامپیوترها و اتصال به اینترنت در شبکه بی سیم را بیان خواهیم کرد و نحوه بکارگیری اتصال به اینترنت بصورت **Dial up** و اشتراک گذاری با سایر کامپیوترها را ذکر می کنیم. در پایان نحوه صرفه جویی در زمان و هزینه در شبکه بی سیم بیان شده است.

8-5- خلاصه فصل

Router ها ابزاری خیلی مفید در شبکه **LAN** هستند در این فصل درباره استفاده مفیدتر از **Router** و بکارگیری آن در شبکه و نحوه اتصال بحث گردید . همچنین در خصوص تغییر بعضی از تنظیمات جهت استفاده **ISP** برای اتصال شبکه به اینترنت نیز مسائلی مطرح گردید با مطالبی که آموختید اکنون قابلیت به شتراک گذاری اینترنت در شبکه را دارید در پایان نیز امکان استفاده از **ICS** در سیستم عامل ویندوز **98SE** و **ME** و نحوه تنظیم آن را بیان نمودیم.

9-آماده سازی اینترنت

در این فصل داریم

- 1-9- تنظیمات **E-mail**
- 2-9- مرور صفحات **web**
- 3-9- اضافه کردن امکانات پیام های فوری
- 4-9- پیدا کردن آدرس **IP**
- 5-9- تست توان عملیاتی یا **Throughput**
- 6-9- تنظیم کردن **E** یا **PPP**

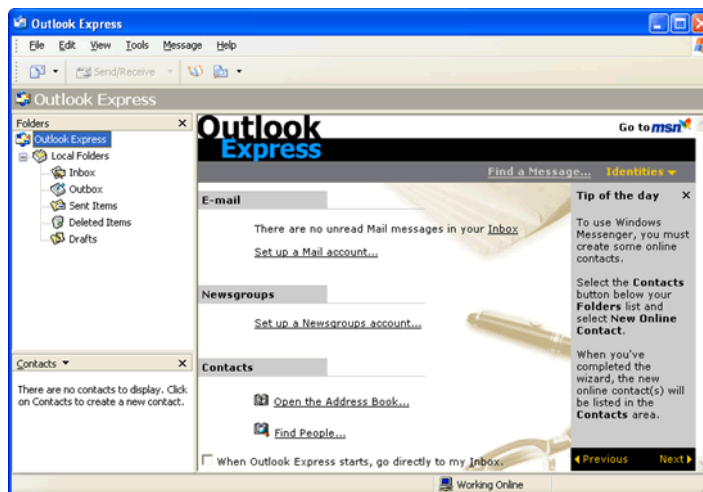
اکنون لازم است منابع و برنامه هایی که روی شبکه بی سیم نصب نمائید . نرم افزارها و برنامه هایی که هر روز مورد استفاده هستند فرستادن **e-mail** مرورگر **web** و پیام های سریع تنها ذره ای از کارهایی است که می توان در شبکه های بی سیم انجام داد.

در اینجا درباره نصب چیزهایی که بعضی وقت ها نصب آنها مشکل بوده و استفاده از آنها باعث راحتی اجرای شبکه می شود بحث خواهیم نمود همچنین نحوه تنظیم **E** یا **point – ppp to-point protocol over Ethenet** را شرح خواهیم داد.

1-9- تنظیمات E-mail

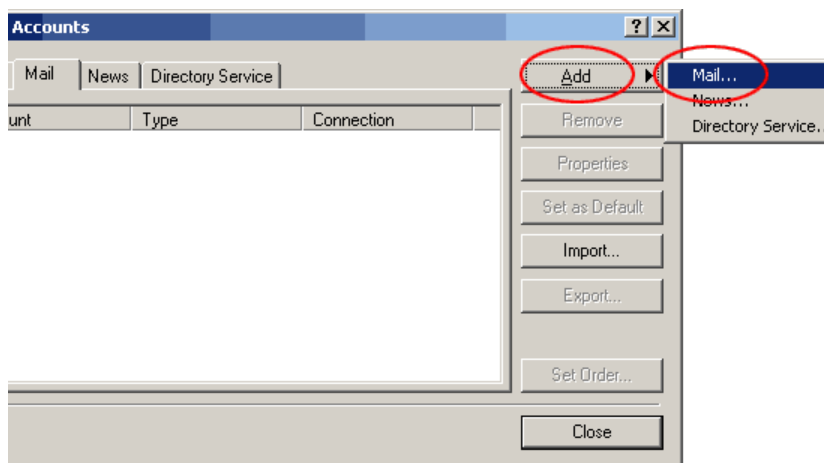
تنظیمات **e-mail** به این صورت است که ابتدا لازم است نامی را برای **client** یا مشتری وارد نمائیم تا بوسیله آن گیرنده مشخص شود. بعد از آن لازم است نام کاربر و رمز تنظیم و نام **server** که **e-mail** بر روی آن ایجاد شده وارد کنیم ما برای این مراحل از برنامه **Outlook Express** که عمومیت بیشتری دارد استفاده می کنیم برای تنظیمات **e-mail** مراحل اساسی زیر را طی می کنیم.

1- اولین قدم ایجاد یک اعتبار یا **Account** جدید است این کار توسط گزینه **Accounting** از منوی **Tools** برنامه **Outlook Express** انجام می شود (شکل 1-9).



شکل 1-9

2- **Add+mail** را انتخاب کنید (شکل 2-9).



شکل 2-9

3- در قسمت **Internet setup Launch** نام افرادی که می توانند هنگام رسیدن **email** مشاهده کنند را وارد کنید سپس دکمه **Next** را بزنید (شکل 3-9).



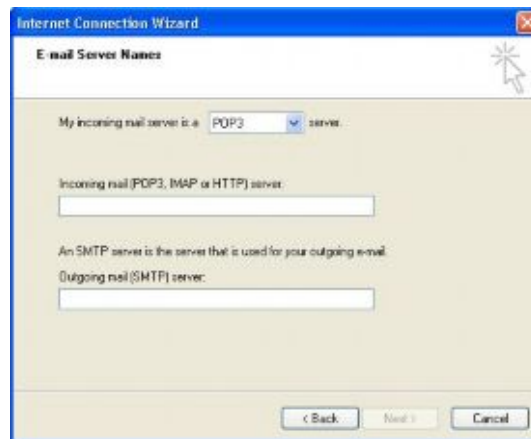
شکل 3-9

5- آدرس **E-mail** خود را وارد کرده و دکمه **Next** را می زنیم (شکل 4-9).



شکل 4-9

5- حال آدرس **server** موجود در **ISP** را وارد کنید **mail server** , **Email** های رسیده را دریافت و ذخیره می کند سرویس دهنده **STP(Simple Mail Transfer Pritocol)** بعنوان سرویس دهنده خارجی است که توسط آن می توان تمام **mail** های فرستاده شده را در دست گرفت مجدداً بکار برد. اگر توسط یک خط تلفن **dial-up** به یک ارتباط اینترنتی پهن باند متصل شده باشید . یا ممکن است برای فرستادن **mail**ها از سرویس دهنده **SMTP** قدیمی استفاده نمائید. تهیه کننده سرویس پهن باند شامل یک اعتبار **E-mail** با سرویس آن می باشد. اما ممکن است شما نخواهید با استفاده از اعتبار **dial-up** بصورت همیشه استفاده کنید و یا اینکه ممکن است بخواهید از آن در مسافرت نیز استفاده کنید.



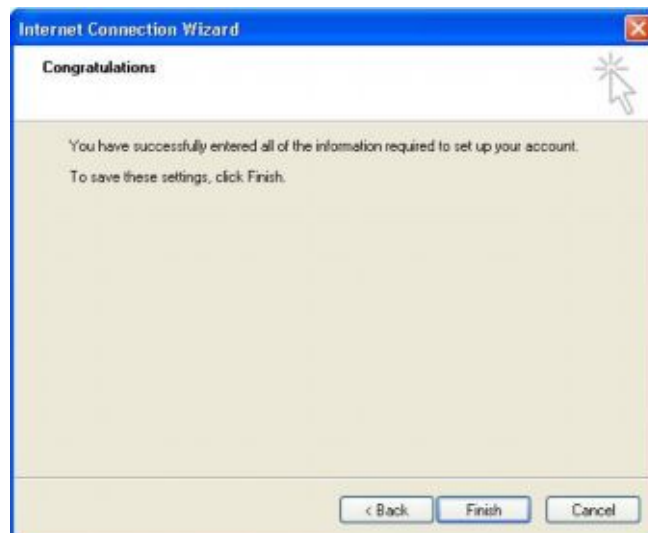
شکل 5-9

7- در جعبه محاوره **account name** نام کاربری که توسط **ISP** ایجاد شده را وارد کنید. (عموماً آن قسمتی از آدرس **e-mail** که قبل از **@** قرار دارد به عنوان **username** بکار می رود) سپس نیاز به وارد کردن کلمه رمز خواهید بود با انتخاب گزینه **Remember Password** دیگر نیازی به وارد کردن کلمه رمز در هر زمان نخواهید داشت.



شکل 6-9

7- روی دکمه **Finish** کلیک کنید تا عملیات **setup** پایان پذیرد (شکل 7-9) اگر ارتباط اینترنت شما فعال باشد با فشار دادن کلید **F5** می توانید بصورت میانبر سرویس ارسال و دریافت **e-mail** را فعال کنید.



شکل 7-9

نکته:

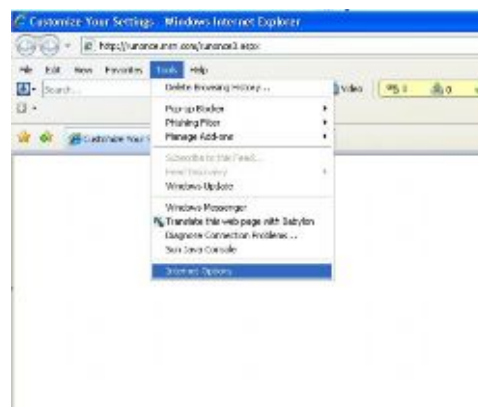
اگر کسی از یک ارتباط **dial-up** استفاده می کند اما می خواهد با یک مودم پهن باند روی شبکه بی سیم اشتراک شود ممکن است نیاز به ترکیب سرویس **mail** با ارتباط قدیم شود و از سرویس **SMTP** با استفاده از مودم پهن باند استفاده کند از نظر امنیتی تعدادی از **ISP**ها اجازه دسترسی به سرویس **mail** با استفاده از **SMTP** نمی دهد.

9-2- مرور صفحات web

فرض می کنیم که شما از طریق **dial up** به اینترنت وصل شده اید ولی می خواهید کامپیوتری که به اینترنت وصل شده را بین سایر کامپیوترهای شبکه بی سیم اشتراک سازی کنیم هر کامپیوتر موجود در شبکه می تواند به وسیله **router** یا توسط ارتباط مستقیم یکی از کامپیوترها با استفاده از خاصیت اشتراک سازی ارتباط اینترنتی یا **ICS** به اینترنت دسترسی داشته باشد.

برای تنظیم مرورگر **web** لازم است هیچ ارتباطی با اینترنت نداشته باشید برای این منظور مراحل زیر را طی می کنیم:

1- منوی **Tools** گزینه **Internet options** را انتخاب کنید (شکل 8-9).



شکل 8-9

2- روی دستگیره **Connections** کلیک کنید (شکل 9-9).



شکل 9-9

3- گزینه **Never dial a connection** را انتخاب کنید اگر مودم روی کامپیوترتان بصورت **internet** نصب شده باشد می توانید **Dial whenever a Network connection is not present** انتخاب نمایید.

9-3- اضافه کردن امکانات پیام های فوری

پیام فوری یا **IM** ابزار ساده برای **chat** می باشد که می توان روی شبکه بی سیم بکار برد برای ایجاد ارتباط سریع و آسان در شبکه خانگی یا اداری نیازی به ارسال یا دریافت **e-mail** نیست شبکه بی سیم روشی کامل ایجاد می کند که می توان با سرعت زیاد پیام ها را بین کاربران مبادله نماید.

ایستگاه های کاری **IM** نیاز به اینترنت دارند اما شما اکنون یک ارتباط را روی شبکه بی سیم اشتراکی کرده اید بنابراین هر کامپیوتر می تواند از نرم افزار **IM** شخصی استفاده می کند و می توان از نرم افزار برای **chat** با ارتباط شخصی استفاده نمود.

ویندوز **XP** دارای یک **IM** ایستگاه کاری بنام **windows Messenger** می باشد **IM** ایستگاه کاری که می توان بکار برد در جدول زیر تعدادی از آنها بیان شده است.

جدول 9-1 معرفی نرم افزار و سایتهای مربوطه

IM Client	سایت برای Download
Widows Messenger	Messenger.msm.com
Aol Instant Massenger	www.aim.com
ICQ	www.icq.com
YahooMessenger	Messenger.yahoo.com

با نصب هر یک از نرم افزارهای **IM** بطور مشابه می توان استفاده نمود.

1- **IM** ایستگاه کاری را **Download** کنید.

2- برنامه **IM** را نصب کنید.

3- افرادی را که می شناسید نامشان را در گروهی وارد کنید.

حال می توانید برای هر کسی با برنامه **IM** پیغام بفرستید باید در نظر داشته باشید که برنامه های **IM** تنها برای ارتباط بین کاربرانی که از نرم افزار مشابه استفاده می کنند بکار می رود.

9-4- پیدا کردن آدرس IP

ممکن است بخواهید روی شبکه بی سیم آدرس **IP** خود را بدانید برای نمونه وقتی یک بازی تحت شبکه را باز می کنید یا در بخش آخر تحقیق وقتی از برنامه ای به نام **Qcheck** که سرعت شبکه بی سیم در تبادل اطلاعات استفاده می شود نیاز است که شما آدرس **IP** را بدانید برای منظور داریم.

9-4-1- در ویندوز 98 یا ME

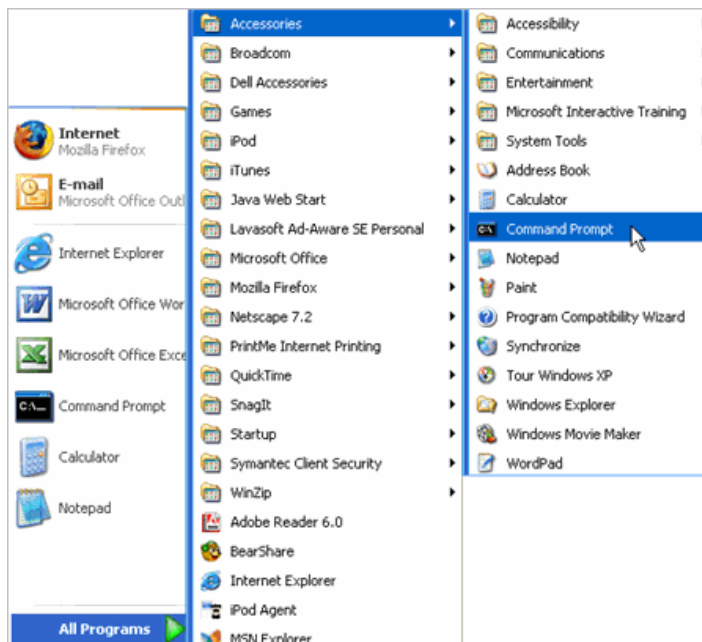
1- از **start** روی گزینه **Run** کلیک کنید.

2- در **open** دستور **winIpconfig** را تایپ کنید این کار را می توان با نوشتن **cmd** در قسمت **open** پنجره ای ظاهر شده در خط فرمان دستور **ipconfig** را وارد کنید.

3- در این حالت باید لیست **IP** آدرس را ببینید. اگر آدرس **IP** را مشاهده نکردید روی منوی **Pull Down** کلیک کنید و سپس کارت شبکه بی سیم را انتخاب کنید.

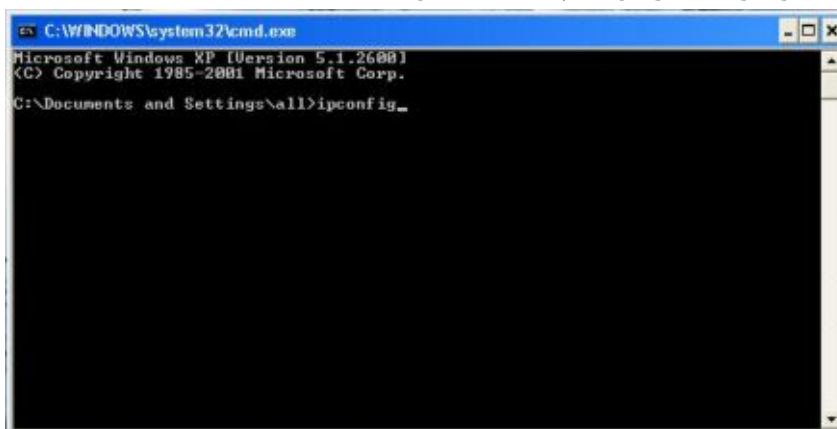
9-4-1- در ویندوز XP یا 2000

1- مراحل زیر را طی کنید Command prompt → Accessories → All programs → start (شکل 9-10)



شکل 9-10

2- دستور Ipconfig را در خط فرمان تایپ کنید (شکل 9-11).



شکل 9-11

بعد از اجرای دستور فوق می توانید آدرس IP کارت شبکه خود را ببینید.

9-5- تست توان عملياتى يا Throughput

نرخ عبور داده ها روى هر شبكه سيمى يا بى سيمى به چند اصل اساسى بستگى دارد. اين اصول به ترتيب عبارتند از

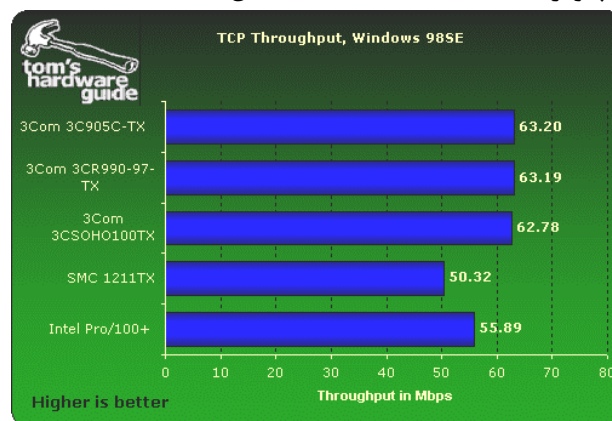
برخورد داده ها در هنگام تبادل اطلاعات بين كامپيوترها دوم اينكه افزايش محدود در بين كامپيوتر يا **Access Point** يا ساير كامپيوترها باعث کاهش انتقال داده ها خواهد شد.

نرخ عبور داده ها را مى توان با استفاده از نرم افزارهاى خاص سنجيد از قبيل برنامه رايگان **Qcheck** كه با نصب روى دو كامپيوتر مى توان نرخ عبور داده را تست نمود.

به عنوان نمونه در زير برنامه **Qcheck** نشان داده شده است با ترتيب بيان شده مى توان نرخ توان عملياتى را تست نمود.

1- برنامه را از سايت www.nefig.com دانلود نماييد.

2- برنامه را روى يکى از كامپيوترهاى شبكه نصب كنيد (شکل 9-12).

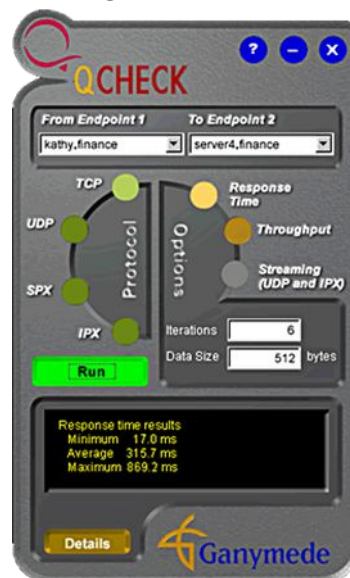


شکل 9-12

3- برنامه را روى يکى ديگر از كامپيوترها نصب كنيد.

4- برنامه را روى هر دو كامپيوتر اجرا كنيد (لازم است روى هر دو كامپيوتر برنامه **Qcheck** اجرا شود).

5- روى دكمه **Throughput** كليك كنيد تا عمل تست شروع شود (شکل 9-13).



شکل 9-13

برنامه **Qchech** بسته های داده را بین دو کامپیوتر می فرستد و زمان ارسال و دریافت انتقال را ضبط می کند. که با سه بار کلیک روی **Throughput** میانگین نتایج اعداد بدست آمده نتیجه توان عملیاتی شبکه را مشخص می کند.

9-6- تنظیم کردن E یا ppp

اکثر **ISP** های پهن باند از یک تکنولوژی بنام پروتکل نقطه به نقطه یا **point-to-point** روی شبکه های **Ethernet** استفاده می کنند این پروتکل باعث ایجاد امنیت دسترسی به ارتباط پهن باند خواهد شد.

اضافه کردن امنیت روی شبکه نیاز به مقداری کاری زیاد دارد.

نکته:

پروتکل نکته به نکته یا **ppp** پروتکل مشترکی است که در ارتباطات **dial-up** اینترنتی استفاده می شود. اگر شما از یک مودم **dial-up** برای اتصال به اینترنت استفاده می کنید به احتمال بیشتر این عمل شما با استفاده از پروتکل **ppp** صورت می گیرد.

اکثر **Router** های شبکه های محلی از یک خصوصیات که به صورت دستی تنظیم میشود باعث ایجاد پروتکل نکته به نکته در اتصال به اینترنت میشود استفاده می کنند برای تمام کاربران لازم است تا با وارد کردن نام کاربری و کلمه رمز و تأیید اعتبار آنها ارتباط با اینترنت را برقرار کنند تعداد خیلی کمی از تولیدکنندگان **Router** دارای این خاصیت هستند اما بعضی از این سازندگان با استفاده از منوی **wizard** این کار را انجام می دهند مانند **Netgear Mr314**.

در شکل 9-20 برنامه **wizard** برای **Router** نوع **Netgear** نشان داده شده است که برای تنظیمات اصلی سخت افزار بکار می رود.



شکل 9-20

10- رفع عیب اتصالات بی سیم (Troubleshoot wireless connection)

در این فصل داریم

- 10-1- آیا درایورهای شبکه از نوع متداول و بروز هستند؟
- 10-2- تشخیص کارتهای شبکه معیوب
- 10-3- اشکالات شبکه ترکیبی ویندوز 98 و ویندوز 2000
- 10-4- پیکربندی سودمند خطاها
- 10-5- توقف یا hangup فایروال
- 10-6- اشکالات چاپگر
- 10-7- سایر اشکالات رایج
- 10-8- خلاصه فصل

نحوه طراحی شبکه بی سیم در بروز اشکالات چندان مهم نیست. این نوع اشکالات نوعاً باعث افت کارایی و گاهی عدم کارت شبکه می شود.

10-1- آیا درایورهای شبکه از نوع متداول و به روز هستند؟

- 1- دیروز تمام برنامه های کاملاً درست کار می کردند ولی امروز هیچ برنامه ای کار نمی کند
 - 2- یکی از ماشین ها کاملاً شبیه سایر کامپیوترها پیکربندی شده اند ولی به شبکه وصل نمی شود.
 - 3- یکی از کامپیوترها به اینترنت دسترسی دارد ولی سایر کامپیوترها موجود در شبکه نمی توانند از آن استفاده کنند اکثر مواقع با انجام موارد زیر اشکال شبکه را خواهید یافت
 - اگر از بروز شدن درایورها مطمئن شدید.
 - اگر از تنظیمات پیکربندی شما به روی کامپیوترهای شبکه استفاده کردید.
 - اگر از امنیت ارتباط های شبکه مطمئن شدید.
- در این صورت باید شکل شبکه شما حل شده باشد.
- لازم است بدانید رفع عیب شبکه نیاز به بردباری و بررسی پایه ای و اصولی شبکه دارد.
- آیا درایورهای شبکه از نوع متداول و رایج هستند؟

استفاده از درایورهای قدیمی ممکن است باعث خرابی شبکه به مرور زمان شوند.

متأسفانه هر دوی سخت افزار جدید شبکه بی سیم و سیستم عامل های جدید همیشه با یکدیگر عرضه می شوند این کار باعث می شود که کاربران با مشکل بزرگی در استفاده سخت افزار شبکه بی سیم با سیستم عامل جدید که ممکن است سخت افزارهای قدیمی را پشتیبانی نکند روبرو خواهند شد.

وقتی سیستم عامل برای اولین بار عرضه شد حتی امروزه نیز اکثر سازندگان کارت های شبکه بی سیم را از نظر نرم افزار نصب سخت افزارها را پشتیبانی نمی کند بنابراین اکثر فروشندگان تجهیزات شبکه بی سیم با ویندوز 2000 که از ویندوز XP پایه ای تر و قدیمی تر است استفاده می کنند.

تعدادی از ویندوز XP برای استاندارد 802.11 b استفاده می کنند که ویندوز XP قابلیت ویندوز 2000 که اکثر درایورهای سخت افزاری را پشتیبانی می کند را ندارند.

ویندوز xp قابلیت شناسایی درایورها را ندارد و نمی توان توسط این سیستم عامل از تمام خصوصیات کارت ها استفاده نمود.

در پایان مطمئن شوید که سخت افزارهای کارت شبکه توسط سیستم عامل پشتیبانی می شود یعنی قبل از خرید با مراجعه به سایت های فروشندگان از نظر پشتیبانی توسط جدیدترین سیستم عامل مطمئن شوید.

10-2- تشخیص کارت های شبکه معیوب

اگر درایورها نصب شما بروز هستند ولی نمی توانید برای اتصال به شبکه توسط کارت شبکه بی سیم استفاده کنید ممکن است امواج رادیویی مناسب نباشد یا اینکه سخت افزار شما مناسب نیستند.

برای رفع این مشکلات سعی کنید کارت های شبکه بی سیم را روی یک کامپیوتر که دارای ارتباط با شبکه هستند مجدداً نصب کرده و روی آن کامپیوتر تست کنید اگر باز نتوانستید ارتباط برقرار کنید روی یک مدل

USB امتحان کنید اگر باز نتوانستید ارتباط ایجاد کنید ممکن کارت شبکه شما تقلبی باشد که در آن صورت می توانید کارت شبکه را به شرکت سازنده عودت دهید.

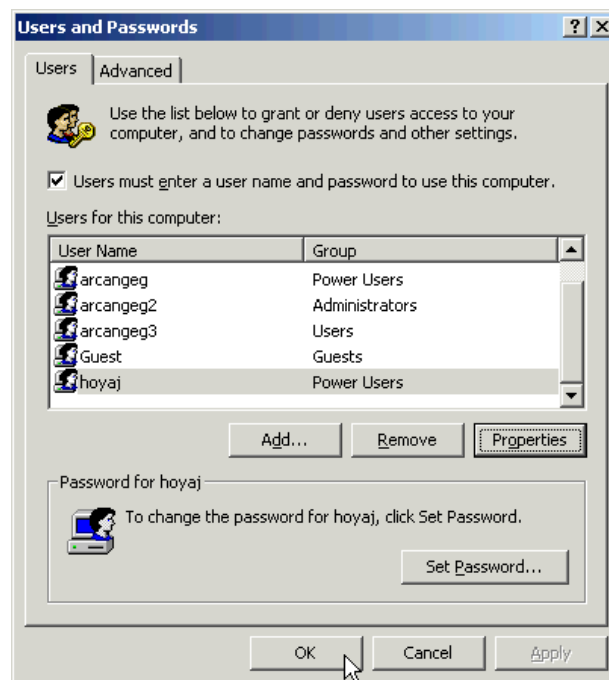
10-3- اشکالات شبکه ترکیبی ویندوز 98 و ویندوز 2000

اکثر افرادی که در شبکه کامپیوتری خود را ترکیب سیستم عامل ویندوز 98 و ویندوز 2000 با اشکالاتی مواجه می شوند بزرگترین اختلاف این سیستم عامل ها وجود یک سطح امنیتی در ویندوز 2000 است که در سایر سیستم عامل ها وجود ندارد این اختلاف باعث می شود که هنگام ارتباط ویندوز 98 به ویندوز 2000 اشکال بوجود آید.

برای درک بهتر این موضوع آن را با مثالی شرح می دهیم کامپیوتری که ویندوز 2000 در آن نصب شده است می تواند براحتی تمام فایل ها و چاپگرهای اشتراکی شده را در یک کامپیوتر با سیستم عامل **window 98SE** را ببیند اما بر عکس موضوع درست نیست. علت چیست؟ ویندوز 2000 برای ارتباط با شبکه و منابع اشتراکی شده درخواست وارد کردن نام کاربری و رمز ورود دارد.

برای رفع این مشکل و ایجاد ارتباط مفید و آسان با کامپیوتر سیستم عامل ویندوز 2000 مراحل زیر را انجام می دهیم.

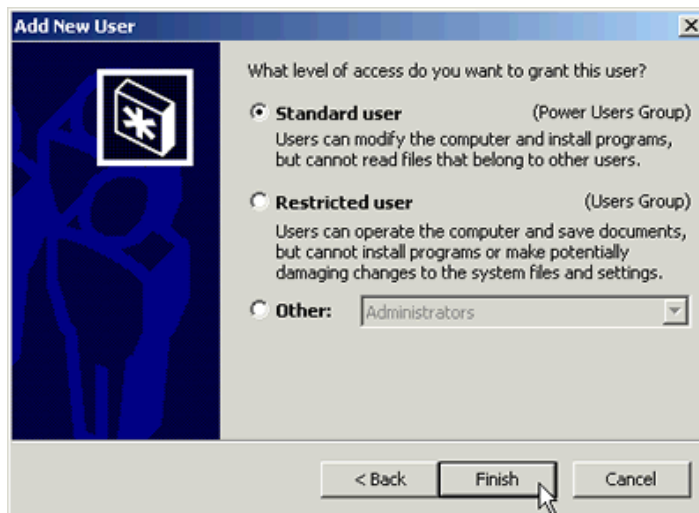
1- از **start → setting → control panel → users and password** روی دکمه **Add** کلیک کنید.



شکل 1-10

2- نامی را وارد کنید و سپس روی دکمه **Next** کلیک کنید.

3- کاربری که مجوز نصب برنامه ها روی این کامپیوتر را دارد انتخاب کنید می توان با انتخاب گزینه **Restricted user** (محدود کردن کاربران) نصب برنامه ها را توسط کاربران بر روی کامپیوتر محدود نمود مهمترین حالت این است که می توان مجوزهای استاندارد را به کاربران انتخاب نمود. در پایان روی دکمه **Finish** کلیک کنید.



شكل 2-10

4- كاربران ويندوز 95/98 يا Me برائى اتصال به شبكه نياز به انتخاب گزينه Login از منوى start و وارد كردن نام كاربرى و رمز عبور دارند تا بتوانند از فايل هاى اشتراكى و چاپگرهاى روى كامپيوتر ويندوز 2000 استفاده نمايند.

توسط ويندوز نصب شده روى كامپيوترها مى توان با هر يك از كامپيوترها ارتباط پيدا كرد و فايل هاى اشتراكى را مرور نمود. در بخش بعد اشكالات ارتباطى خاص شبكه هاى بى سيم را بيان خواهيم كرد.

4-10- پيكربندى سودمند خطاها

زمانيكه متوجه شديد كه شبكه شما كار نمى كند اولين قدم امتحان تنظيمات مفيد پيكربندى هر يك از كارت هاى شبكه است هر كارت شبكه كه در آن چراغ سبز روشن نباشد مشخص مى كند كه به شبكه بى سيم وصل نيست.

در اين قسمت درباره سه نوع اشكال عمده در استاندارد شبكه 802.11 b بيان شده است بنا بر اين برائى تست خرابى لازم است ابتدا اين سه حالت را بررسى كنيد.

1- مطمئن شويد كه شبكه شما به حالت Ad-Hoc تنظيم شده باشد اين در حالتى كه شبكه شما داراى Access Point نيست يا اينكه در حالت Infrastructure تنظيم كرده ايد و اين در موقعى است كه شما از Access Point استفاده مى كنيد.

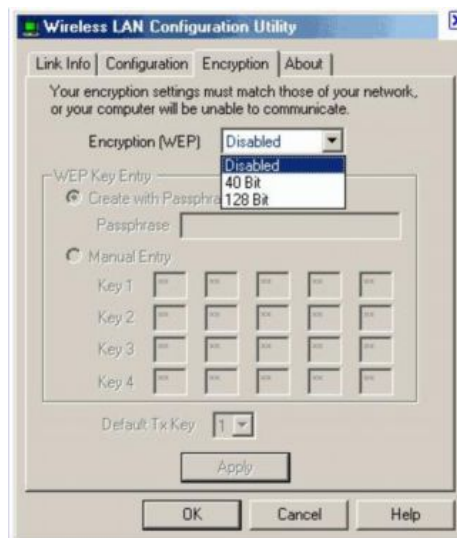
2- اگر شما از روش رمزگذارى استفاده مى كنيد بايد مطمئن شويد كه تمام كامپيوترهاى موجود در شبكه و Access Point از نظر رمزگذارى داراى سطح يكسانى باشند (شكل 3-10) اگر يكى از كارت هاى شبكه با سيم در حالت 64 بيتى رمزگذارى شده باشد و سايرين با 128 بيت رمزگذاى شوند در اين حالت ارتباطى وجود نخواهد داشت



شکل 3-10

3- سرویس شناسایی یا شکل 3-10

3- سرویس شناسایی یا **SSID (Service Set Identifier)** را چک کنید تا اینکه در تمام کامپیوترها این سرویس یکسانی باشند مانند رمزگذاری اگر یکی از ماشین ها دارای تنظیم **SSID** متفاوتی داشته باشد مطمئناً نمی تواند به شبکه بی سیم وصل شود.



شکل 4-10

می توان با انتخاب گزینه **Any** برای **SSID** روی کارت های شبکه امکان ایجاد ارتباط هر **SSI** در شبکه را ایجاد نمود.

زمانیکه نرم افزار پیکربندی را روی هر یک از کارت های شبکه بدرستی انجام دادید مطمئن شوید که کامپیوترهای شما می توانند به شبکه وصل شوند.

5-10- توقف یا hangup فایروال

بعضی مواقع وجود **Firewall** باعث انجام کارهای مفیدی می شود چنانچه قبلاً گفتیم یک **Firewall** کمک می کند تا افراد غیر مجاز نتوانند به شبکه دسترسی داشته باشند. با هم بودن **Firewall** در داخل ویندوز **XP** بهتر از سایر نرم افزارهای **Firewall** می باشد. زیرا نصب **Firewall** موجود در ویندوز کاملتر و صحیح بوده و سازگار می باشد ولی ممکن است نصب غیر صحیح **Firewall** باعث از کار افتادن شبکه شود. در اولین مرحله هر چند لازم است یک روی هر یک از کامپیوترهای شبکه نصب شود. اما اکثر افراد دوست دارند **Router** خریداری کنند که در آن وجود دارد در این حالت دیگر نیازی به نصب یک نرم افزار **Firewall** روی هر یک از کامپیوترهای شبکه نیست. **Firewall** موجود در داخل **Router** باید بطور کامل شبکه را از نفوذ هکرها یا افرادی که بدون مجوز می خواهد از طریق اینترنت به شبکه وارد شوند محافظت نماید.

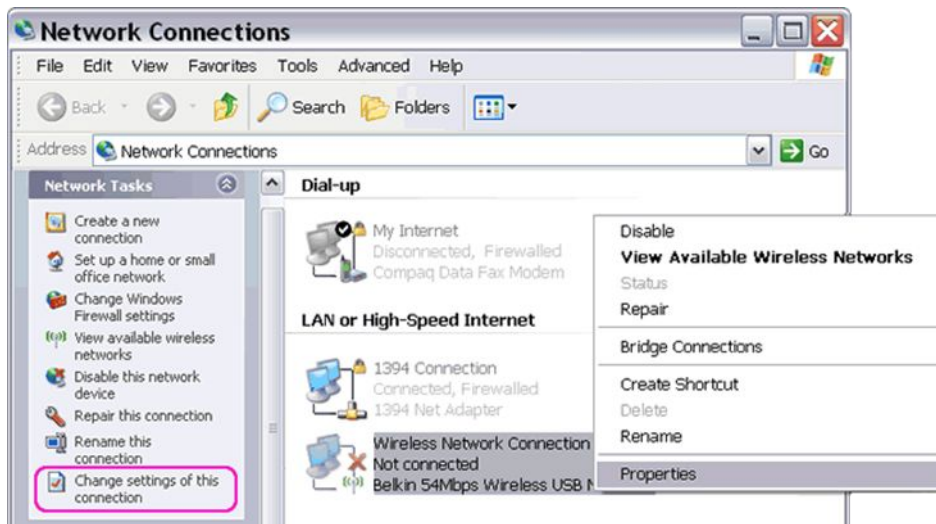
اگر سیستم عامل روی کامپیوتر شما **windows XP** است نحوه غیر فعال کردن **Firewall** در موقع ایجاد مشکل در شبکه به صورت زیر است.

1- از **desktop** گزینه **My Network Place** را باز کنید (شکل 5-10).



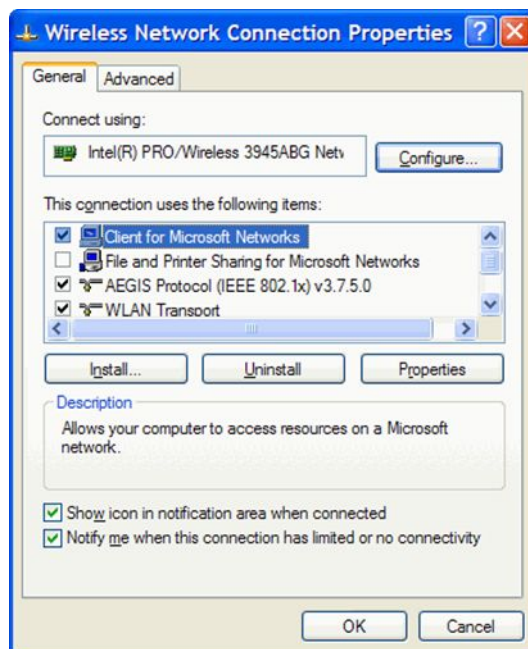
شکل 5-10

2- روی گزینه **Wireless Network Connection** راست کلیک کرده و سپس گزینه **properties** را انتخاب کنید (شکل 6-10).



شکل 10-6

3- روی دستگیره Advance کلیک کنید (شکل 10-7).



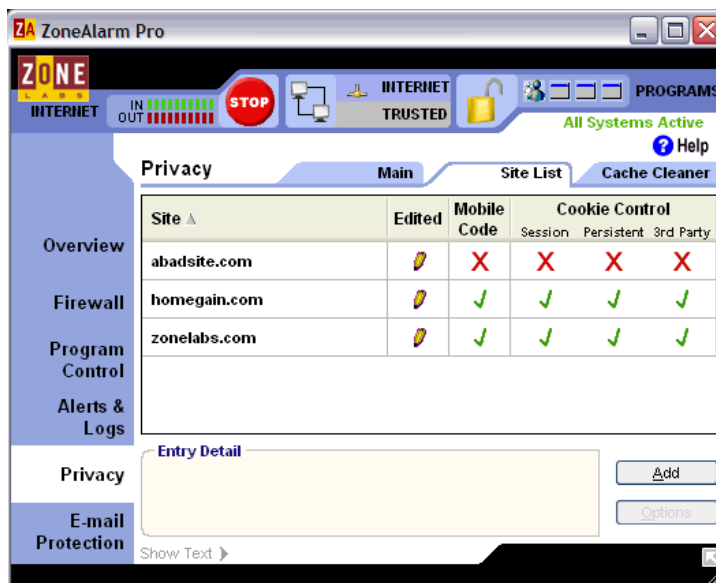
شکل 10-7

3- گزینه "protect my computer and network by limiting or preventing access to this computer from the internet"

4- روی دکمه ok کلیک کنید تا پنجره بسته شود.

اگر از یک Firewall شخصی از قبیل Zone Alarm استفاده می کنید (www.Zonelabs.com) می توانید نرم افزار را طوری تنظیم کنید که کامپیوترهای موجود در شبکه را شناسایی و تشخیص دهد. می توان این برنامه را از سایت ذکر شده دانلود کرده و نصب نمود بعد از اجرای برنامه Zone Alarm می توان با تنظیمات بیان شده اجازه کار در شبکه پیدا کرد.

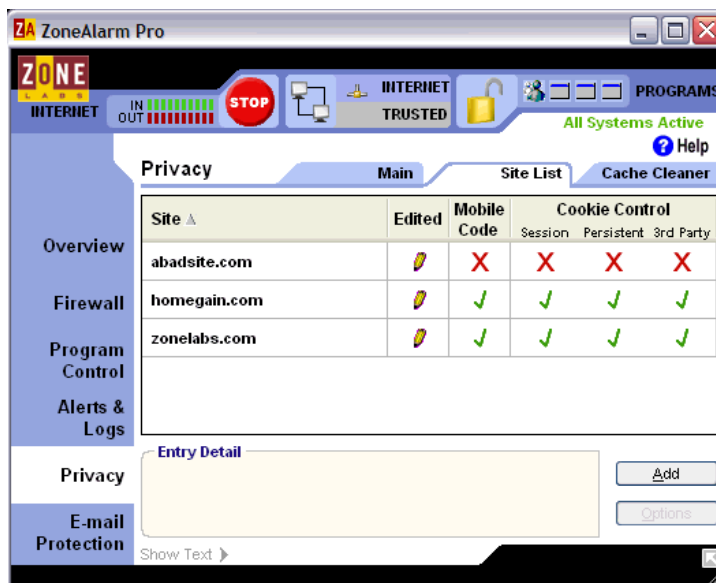
1- روی دکمه Decurity کلیک کنید (شکل 10-8).



<http://technologycurrent.com/wp-content/uploads/2008/07/zonealarm1.png>

شکل 8-10

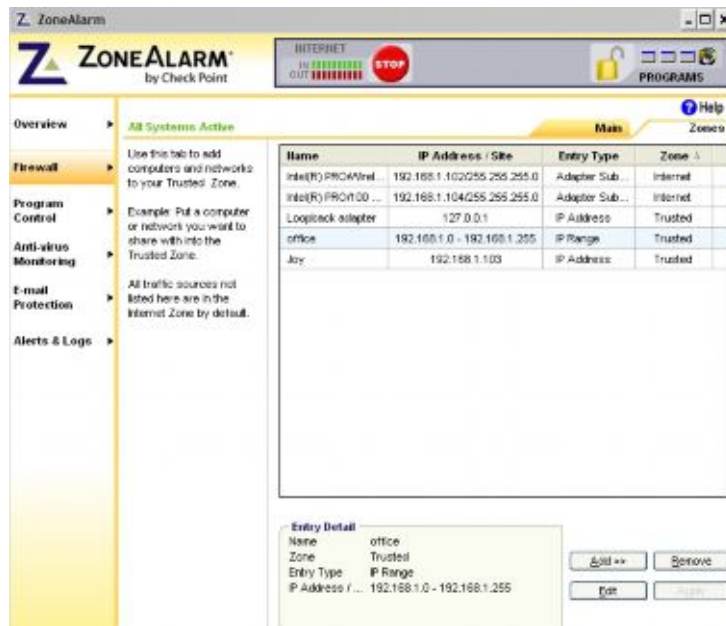
2- روی دکمه **Advanced** کلیک کنید (شکل 9-10).



<http://technologycurrent.com/wp-content/uploads/2008/07/zonealarm1.png>

شکل 9-10

3- کارت شبکه را انتخاب کنید (شکل 10-10).



<http://attachments.techguy.org/attachments/124993d1201383695/zone-alarm-firewall-zones.jpg>

شکل 10-10

روی دکمه Add و سپس روی دکمه Apply کلیک کنید.

10-6- اشکالات چاپگر

مشکلات استفاده از چاپگر اکثر مواقعی رخ می دهد که در محیط ها سیستم عامل اختلاطی بوجود آید یعنی یک نرم افزار نصب چاپگر روی یک از کامپیوترها عیب پیدا کند بهترین کار در چنین مواقعی استفاده از آخرین نسخه نرم افزار نصب در سیستم عامل است هر کامپیوتر نیاز به نصب درایور صحیح جهت دسترسی به چاپگر مشترک دارد.

اگر یک چاپگر در **Network Neighborhood** (در ویندوز 95 و 98) یا **My Network place** **Network place** (در ویندوز XP یا 2000 یا Me) نشان داده نشود مطمئن شوید. که کاربری به شبکه وصل شده و می خواهد به چاپگر اشتراکی شده دسترسی داشته باشد.

10-7- سایر اشکالات رایج

- اگر باز اشکالاتی در شبکه وجود داشته باشد یک تعداد از این اشکالات احتمالی در اینجا بیان می شود
- سعی کنید تمام تجهیزات شبکه بی سیم را در محدود بسته بررسی کنید ممکن است تجهیزاتی در شبکه موجود باشد که خارج از محدود قرار گرفته باشند.
- رمزگذاری بی سیم (WEP) را تا زمانیکه تجهیزات شبکه را تنظیم می کند از حالت فعال خارج کنید.
- آیا می توانید به اینترنت متصل شوید اگر می توانید ولی اگر کامپیوترهای موجود در شبکه نمی توانند به فایل ها و چاپگرهای اشتراکی دسترسی داشته باشند نشان دهنده آن است که این شکل تنظیمات شبکه در ویندوز می باشد.

به اینترنت دسترسی ندارید؟ مودم پهن باندتان را چک کنید آیا هنگام اجرا و بالا آمدن مودم چراغ لینک ISP آن روشن است؟ (اکثر مودم های پهن باند دارای 3 چراغ می باشد که می بایست به ترتیب روشن شوند یکی از چراغ ها برای نمایش ارتباط با شبکه ISP دیگری جهت نمایش وجود ارتباط با شبکه داخلی و یکی از این سه چراغ نمایش وجود برق در مودم می باشد).

اگر در پایان باز موفق نشدید تمام تجهیزات را خاموش کرده و مجدداً روشن کنید ابتدا مودم سپس Router در صورت وجود Access Point و در پایان کامپیوتر را روشن کرده و مطمئن شوید که هر یک از دستگاه ها بعد از راه اندازی مجدد شروع به کار می کنند.

10-8- خلاصه فصل

هر كسى در اجراى ايجاد شبكه ممكن است با مشكلاتى مواجه شود مخصوصاً در اولين مراحل راه اندازى خبر خوب اينكه هنگام بروز مشكل در شبكه هاى بى سيم مثل شبكه هاى سيمى كه كار زيادى بكار مى رود نيست و خبر بد اينكه بعضى وقت ها هنگام بروز مشكل از قبيل تداخل امواج در يك كارت شبكه بى سيم تشخيص آن شكل بوده و باعث از كار افتادن شبكه مى شود.

11- امنیت

در این فصل داریم

- 1-11- منشاء ضعف امنیتی در شبکه های بی سیم و خطرات معمول
- 2-11- امنیت و پروتکل WEP
- 3-11- قابلیتها و ابعاد امنیتی استاندارد 802,11
- 4-11- AUTHENTICATION
- 5-11- Authentication بدون رمزنگاری (Open System Authentication)
- 6-11- Authentication با رمزنگاری RC4 (shared key Authentication)
- 7-11- ضعف در الگوریتم
- 8-11- مقایسه استانداردهای 802,11

11-1- منشأ ضعف امنیتی در شبکه های بی سیم و خطرات معمول

خطر معمول در کلیه ی شبکه های بی سیم مستقل از پروتکل و تکنولوژی مورد نظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار، مبتنی بر استفاده از سیگنال های رادیویی به جای سیم و کابل، استوار است. با استفاده از این سیگنال ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه چندان قدرتمند این شبکه ها، خود را به عنوان عضوی از این شبکه ها جازده و در صورت تحقق این امر، امکان دستیابی به اطلاعات حیاتی، حمله به سرویس دهنده گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره های شبکه با یکدیگر، تولید داده های غیر واقعی و گمراه کننده، سوءاستفاده از پهنای باند مؤثر شبکه و دیگر فعالیت های مخرب وجود دارد. در مجموع، در تمامی دسته های شبکه های بی سیم، از دید امنیتی حقایقی مشترک صادق است - تمامی ضعف های امنیتی موجود در شبکه های سیمی، در مورد شبکه های بی سیم نیز صدق می کند. در واقع نه تنها هیچ جنبه یی چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه های بی سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان گونه که ذکر شد مخاطرات ویژه یی را نیز موجب است.

- نفوذگران، با گذر از تدابیر امنیتی موجود، می توانند به راحتی به منابع اطلاعاتی موجود بر روی سیستم های رایانه یی دست یابند.

- اطلاعات حیاتی که یا رمز نشده اند و یا با روشی با امنیت پایین رمز شده اند، و میان دو گره در شبکه های بی سیم در حال انتقال می باشند، می توانند توسط نفوذگران سرقت شده یا تغییر یابند.
- حمله های DoS به تجهیزات و سیستم های بی سیم بسیار متداول است.
- نفوذگران با سرقت کدهای عبور و دیگر عناصر امنیتی مشابه کاربران مجاز در شبکه های بی سیم، می توانند به شبکه یی مورد نظر بدون هیچ مانعی متصل گردند.
- با سرقت عناصر امنیتی، یک نفوذگر می تواند رفتار یک کاربر را پایش کند. از این طریق می توان به اطلاعات حساس دیگری نیز دست یافت.

- کامپیوترهای قابل حمل و جیبی، که امکان و اجازه ی استفاده از شبکه یی بی سیم را دارند، به راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می توان اولین قدم برای نفوذ به شبکه را برداشت.
- یک نفوذگر می تواند از نقاط مشترک میان یک شبکه یی بی سیم در یک سازمان و شبکه یی سیمی آن (که در اغلب موارد شبکه یی اصلی و حساس تری محسوب می گردد) استفاده کرده و با نفوذ به شبکه یی بی سیم عملاً راهی برای دستیابی به منابع شبکه یی سیمی نیز بیابد.
- در سطحی دیگر، با نفوذ به عناصر کنترل کننده ی یک شبکه یی بی سیم، امکان ایجاد اختلال در عمل کرد شبکه نیز وجود دارد.

11-1-1- برد و سطح پوشش

اولین مبحثی که در مورد امنیت شبکه های بی سیم مهم است این نکته است که ما بدانیم. شبکه ما تا مسافتی کاربرد دارد. شعاع پوشش شبکه ی بی سیم بر اساس استاندارد 802,11 به فاکتورهای بسیاری بستگی دارد که برخی از آنها به شرح زیر هستند

پهنای باند مورد استفاده

منابع امواج ارسالی و محل قرارگیری فرستنده ها و گیرنده ها

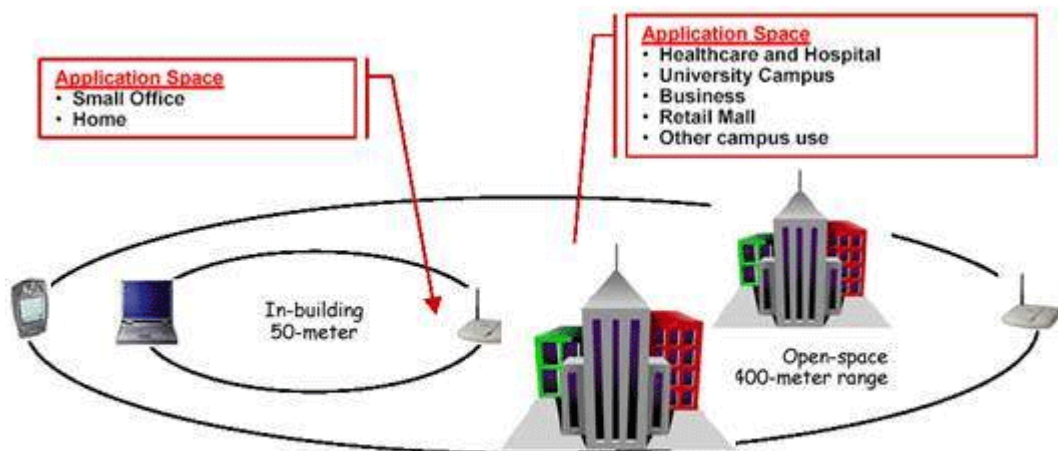
مشخصات فضای قرارگیری و نصب تجهیزات شبکه ی بی سیم

قدرت امواج

نوع و مدل آنتن

شعاع پوشش از نظر تئوری بین 29متر (برای فضاهای بسته ی داخلی) و 485متر (برای فضاهای باز) در استاندارد 802.11 b متغیر است. با این وجود این مقادیر، مقادیری متوسط هستند و در حال حاضر با توجه به گیرنده ها و فرستنده های نسبتاً قدرتمندی که مورد استفاده قرار می گیرند، امکان استفاده از این پروتکل و گیرنده ها و فرستنده های آن، تا چند کیلومتر هم وجود دارد که نمونه های عملی آن فراوان اند. با این وجود شعاع که برای استفاده از این پروتکل (802.11 b) ذکر می شود چیزی میان 50 تا 100متر است. این شعاع عمل کرد مقداریست که برای محل های بسته و ساختمان های چند طبقه نیز معتبر بوده و می تواند مورد استناد قرار گیرد.

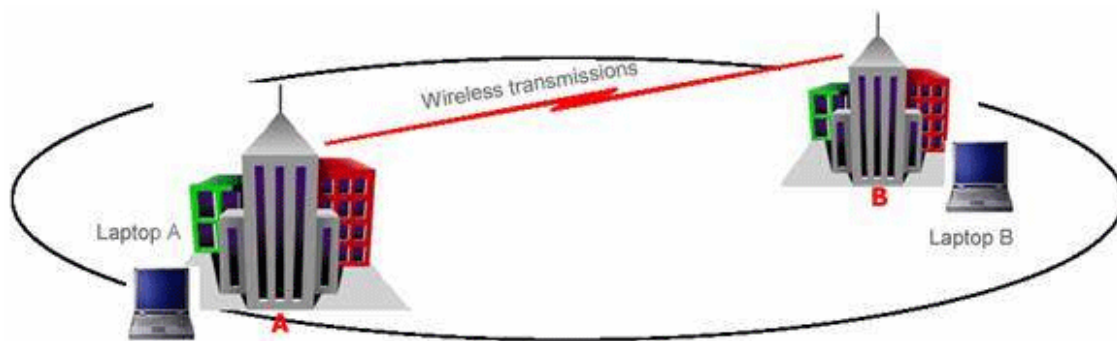
شکل 1-11 زیر مقایسه یی میان بردهای نمونه در کاربردهای مختلف شبکه های بی سیم مبتنی بر پروتکل 802.11 b را نشان می دهد.



شکل 1-11

یکی از عمل کردهای نقاط دسترسی به عنوان سویچ های بی سیم، عمل اتصال میان حوزه های بی سیم است. به عبارت دیگر با استفاده از چند سویچ بی سیم می توان عمل کردی مشابه **Bridge** برای شبکه های بی سیم را بدست می آورد اتصال میان نقاط دسترسی می تواند به صورت نقطه به نقطه، برای ایجاد اتصال میان دو زیر شبکه به یکدیگر، یا به صورت نقطه یی به چند نقطه یا بالعکس برای ایجاد اتصال میان زیر شبکه های مختلف به یکدیگر به صورت همزمان صورت گیرد.

نقاط دسترسی یی که به عنوان پل ارتباطی میان شبکه های محلی با یکدیگر استفاده می شوند از قدرت بالاتری برای ارسال داده استفاده می کنند و این به معنای شعاع پوشش بالاتر است. این سخت افزارها معمولاً برای ایجاد اتصال میان نقاط و ساختمان هایی به کار می روند که فاصله ی آنها از یکدیگر بین 1 تا 5 کیلومتر است. البته باید توجه داشت که این فاصله، فاصله یی متوسط بر اساس پروتکل **802.11b** است. برای پروتکل های دیگری چون **802.11a** می توان فواصل بیشتری را نیز به دست آورد. شکل 2-11 زیر نمونه یی از ارتباط نقطه به نقطه با استفاده از نقاط دسترسی مناسب را نشان می دهد



شکل 2-11

از دیگر استفاده های نقاط دسترسی با برد بالا می توان به امکان توسعه ی شعاع پوشش شبکه های بی سیم اشاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوشش یک شبکه ی بی سیم، می توان از چند نقطه ی دسترسی بی سیم به صورت همزمان و پشت به پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا می توان با استفاده از یک فرستنده ی دیگر در بالای هر یک از ساختمان ها، سطح پوشش شبکه را تا ساختمان های دیگر گسترش داد.

2-1-11- خدمات توزیع

خدمات توزیع عملکرد لازم در همبندی های مبتنی بر سیستم توزیع را مهیا می سازد. معمولاً خدمات توزیع توسط نقطه دسترسی فراهم می شوند. خدمات توزیع در این استاندارد عبارتند از پیوستن به شبکه خروج از شبکه بی سیم

پیوستن مجدد

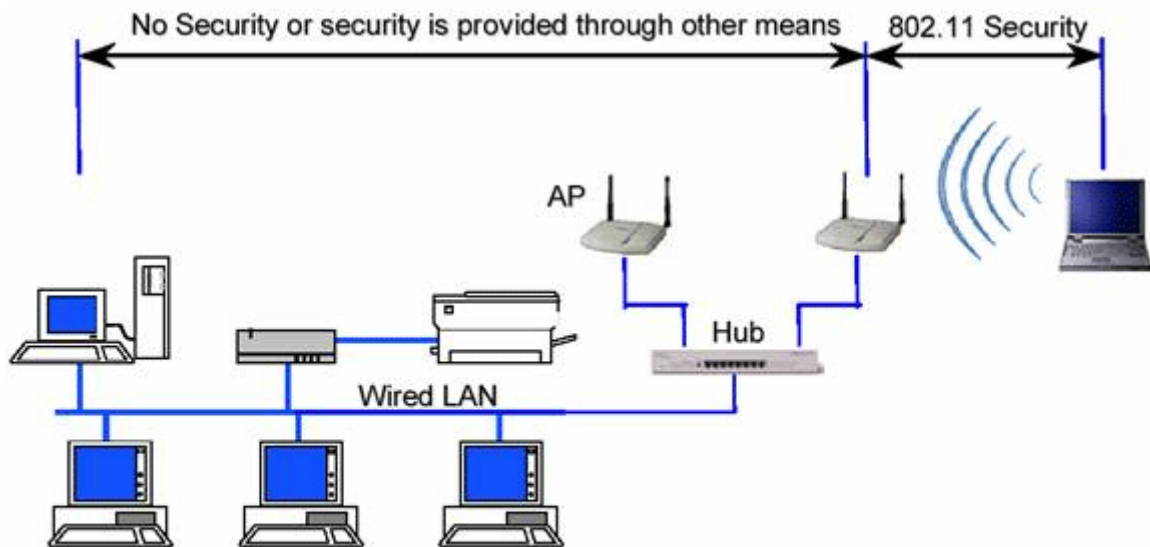
توزیع

3-1-11- مجتمع سازی

سرویس اول یک ارتباط منطقی میان ایستگاه سیار و نقطه دسترسی فراهم می کند. هر ایستگاه کاری قبل از ارسال داده می بایست با یک نقطه دسترسی بر روی سیستم میزبان مرتبط گردد. این عضویت، به سیستم توزیع امکان می دهد که فریم های ارسال شده به سمت ایستگاه سیار را به درستی در اختیارش قرار دهد. خروج از شبکه بی سیم هنگامی بکار می رود که بخواهیم اجباراً ارتباط ایستگاه سیار را از نقطه دسترسی قطع کنیم و یا هنگامی که ایستگاه سیار بخواهد خاتمه نیازش به نقطه دسترسی را اعلام کند. سرویس پیوستن مجدد هنگامی مورد نیاز است که ایستگاه سیار بخواهد با نقطه دسترسی دیگری تماس بگیرد. این سرویس مشابه "پیوستن به شبکه بی سیم" است با این تفاوت که در این سرویس ایستگاه سیار نقطه دسترسی قبلی خود را به نقطه دسترسی جدیدی اعلام می کند که قصد دارد به آن متصل شود. پیوستن مجدد با توجه به تحرک و سیار بودن ایستگاه کاری امری ضروری و اجتناب ناپذیر است. این اطلاع، (اعلام نقطه دسترسی قبلی) به نقطه دسترسی جدید کمک می کند که با نقطه دسترسی قبلی تماس گرفته و فریم های بافر شده احتمالی را دریافت کند که به مقصد این ایستگاه سیار فرستاده شده اند. با استفاده از سرویس توزیع فریم های لایه MAC به مقصد مورد نظرشان می رسند. مجتمع سازی سرویسی است که شبکه محلی بی سیم را به سایر شبکه های محلی و یا یک یا چند شبکه محلی بی سیم دیگر متصل می کند. سرویس مجتمع سازی فریم های 802,11 را به فریم هایی ترجمه می کند که بتوانند در سایر شبکه ها (به عنوان مثال 802,3) جاری شوند. این عمل ترجمه دو طرفه است بدان معنی که فریم های سایر شبکه ها نیز به فریم های 802,11 ترجمه شده و از طریق امواج در اختیار ایستگاه های کاری سیار قرار می گیرند.

2-11- امنیت و پروتکل WEP

از این قسمت بررسی روش ها و استانداردهای امن سازی شبکه های محلی بی سیم مبتنی بر استاندارد IEEE 802.11 را آغاز می کنیم. با طرح قابلیت های امنیتی این استاندارد، می توان از محدودیت های آن آگاه شد و این استاندارد و کاربرد را برای موارد خاص و مناسب مورد استفاده قرار داد. استاندارد 802,11 سرویس های مجزا و مشخصی را برای تأمین یک محیط امن بی سیم در اختیار قرار می دهد. این سرویس ها اغلب توسط پروتکل WEP (Wired Equivalent Privacy) تأمین می گردند و وظیفه ی آنها امن سازی ارتباط میان مخدوم ها و نقاط دسترسی بی سیم است. درک لایه یی که این پروتکل به امن سازی آن می پردازد اهمیت ویژه یی دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه های دیگر، غیر از لایه ی ارتباطی بی سیم که مبتنی بر استاندارد 802,11 است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه ی بی سیم به معنی استفاده از قابلیت درونی استاندارد شبکه های محلی بی سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.



شکل 3-11 محدوده ی عملکرد استانداردهای امنیتی 802,11 (خصوصاً wep) را نشان می دهد.

3-11- قابلیت ها و ابعاد امنیتی استاندارد 802,11

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه های بی سیم بر اساس استاندارد 802,11 فراهم می کند **WEP** است. این پروتکل با وجود قابلیت هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه های بی سیم را به نحوی، ولو سخت و پیچیده، فراهم می کند. نکته یی که باید به خاطر داشت اینست که اغلب حملات موفق صورت گرفته در مورد شبکه های محلی بی سیم، ریشه در پیکربندی ناصحیح **WEP** در شبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می گذارد، هرچند که فی نفسه دچار نواقص و ایرادهایی نیز هست. بسیاری از حملاتی که بر روی شبکه های بی سیم انجام می گیرد از سویی است که نقاط دسترسی با شبکه ی سیمی دارای اشتراک هستند. به عبارت دیگر نفوذگران بعضاً با استفاده از راه های ارتباطی دیگری که بر روی مخدوم ها و سخت افزارهای بی سیم، خصوصاً مخدوم های بی سیم، وجود دارد، به شبکه ی بی سیم نفوذ می کنند که این مقوله نشان دهنده ی اشتراکی هرچند جزئی میان امنیت در شبکه های سیمی و بی سیمی است که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند. سه قابلیت و سرویس پایه توسط **IEEE** برای شبکه های محلی بی سیم تعریف می گردد.

Authentication

Confidentiality

Integrity

Authentication -4-11

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

1-4-11- خدمات ایستگاهی

بر اساس این استاندارد خدمات خاصی در ایستگاه های کاری پیاده سازی می شوند. در حقیقت تمام ایستگاه های کاری موجود در یک شبکه محلی مبتنی بر 802,11 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 شبکه های سیمی، در شبکه های بی سیم قابل اعمال نیست استاندارد 802,11 خدمات هویت سنجی را به منظور کنترل دسترسی به شبکه تعریف می نماید. سرویس هویت سنجی به ایستگاه کاری امکان می دهد که ایستگاه دیگری را شناسایی نماید. قبل از اثبات هویت ایستگاه کاری، آن ایستگاه مجاز نیست که از شبکه بی سیم برای تبادل داده استفاده نماید. در یک تقسیم بندی کلی 802,11 دو گونه خدمت هویت سنجی را تعریف می کند

Authentication Open System

Shared Key Authentication

روش اول، متد پیش فرض است و یک فرآیند دو مرحله ای است. در ابتدا ایستگاهی که می خواهد توسط ایستگاه دیگر شناسایی و هویت سنجی شود یک فریم مدیریتی هویت سنجی شامل شناسه ایستگاه فرستنده، ارسال می کند. ایستگاه گیرنده نیز فریمی در پاسخ می فرستد که آیا فرستنده را می شناسد یا خیر. روش دوم کمی پیچیده تر است و فرض می کند که هر ایستگاه از طریق یک کانال مستقل و امن، یک کلید مشترک سری دریافت کرده است. ایستگاه های کاری با استفاده از این کلید مشترک و با بهره گیری از پروتکلی موسوم به WEP اقدام به هویت سنجی یکدیگر می نمایند. 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 می گردد.

در یک شبکه بی سیم، تمام ایستگاه های کاری و سایر تجهیزات قادر هستند ترافیک داده ای را "بشنوند" در واقع ترافیک در بستر امواج مبادله می شود که توسط تمام ایستگاه های کاری قابل دریافت است. این ویژگی سطح امنیتی یک ارتباط بی سیم را تحت تأثیر قرار می دهد. به همین دلیل در استاندارد 802,11 پروتکلی موسوم به WEP تعبیه شده است که بر روی تمام فریم های داده و برخی فریم های مدیریتی و هویت سنجی اعمال می شود. این استاندارد در پی آن است تا با استفاده از این الگوریتم سطح اختفاء و پوشش را معادل با شبکه های سیمی نماید.

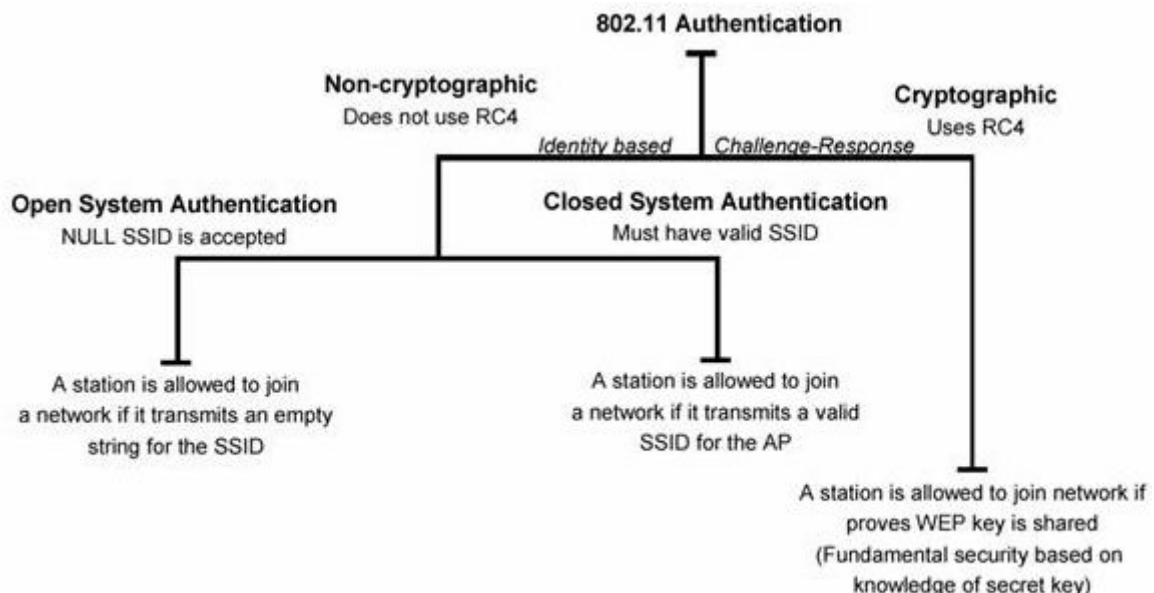
Confidentiality -2-4-11

محرمانه گی هدف دیگر WEP است. این بُعد از سرویس ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه ی محلی بی سیم است.

Integrity -3-4-11

هدف سوم از سرویس ها و قابلیت های WEP طراحی سیاستی است که تضمین کند پیام ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان مخدوم های بی سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه های ارتباطاتی دیگر نیز کم و بیش وجود دارد. نکته ی مهمی که در مورد سه سرویس WEP وجود دارد نبود سرویس های معمول Auditing و Authorization در میان سرویس های ارائه شده توسط این پروتکل است.

استاندارد 802,11 دو روش برای احراز هویت کاربرانی که درخواست اتصال به شبکه ی بی سیم را به نقاط دسترسی ارسال می کنند، دارد که یک روش بر مبنای رمزنگاری است و دیگری از رمزنگاری استفاده نمی کند. شکل زیر شمایی از فرایند Authentication را در این شبکه ها نشان می دهد.



شکل 4-11

همان گونه که در شکل 4-11 نیز نشان داده شده است، یک روش از رمزنگاری RC4 استفاده می کند و روش دیگر از هیچ تکنیک رمزنگاری بی استفاده نمی کند.

11-5- Authentication بدون رمزنگاری (Open System Authentication)

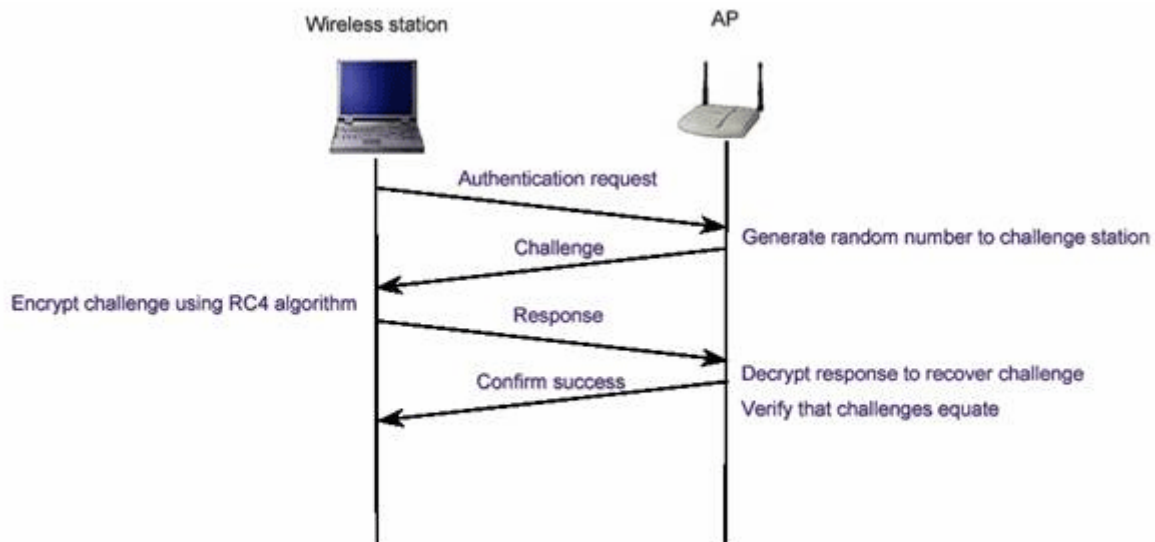
در روشی که مبتنی بر رمزنگاری نیست، دو روش برای تشخیص هویت مخدوم وجود دارد. در هر دو روش مخدوم متقاضی پیوستن به شبکه، درخواست ارسال هویت از سوی نقطه دسترسی را با پیامی حاوی یک **SSID (Service Set Identifier)** پاسخ می‌دهد.

در روش اول که به **Open System Authentication** موسوم است، یک **SSID** خالی نیز برای دریافت اجازه‌ی اتصال به شبکه کفایت می‌کند. در واقع در این روش تمامی مخدوم‌هایی که تقاضای پیوستن به شبکه را به نقاط دسترسی ارسال می‌کنند با پاسخ مثبت روبه‌رو می‌شوند و تنها آدرس آن‌ها توسط نقطه‌ی دسترسی نگاه‌داری می‌شود. به همین دلیل به این روش **NULL Authentication** نیز اطلاق می‌شود. در روش دوم از این نوع، بازهم یک **SSID** به نقطه‌ی دسترسی ارسال می‌گردد با این تفاوت که اجازه‌ی اتصال به شبکه تنها در صورتی از سوی نقطه‌ی دسترسی صادر می‌گردد که **SSID** ارسال شده جزو **SSID**های مجاز برای دسترسی به شبکه باشند. این روش به **Closed System Authentication** موسوم است.

نکته‌ی که در این میان اهمیت بسیاری دارد، توجه به سطح امنیتی است که این روش در اختیار ما می‌گذارد. این دو روش عملاً روش امنی از احراز هویت را ارائه نمی‌دهند و عملاً تنها راهی برای آگاهی نسبی و نه قطعی از هویت درخواست‌کننده هستند. با این وصف از آن جایی که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران کم‌تجربه و مبتدی، به شبکه‌هایی که بر اساس این روش‌ها عمل می‌کنند، رخ می‌دهد، لذا این دو روش تنها در حالتی کاربرد دارند که یا شبکه‌ی در حال ایجاد است که حاوی اطلاعات حیاتی نیست، یا احتمال رخداد حمله به آن بسیار کم است. هرچند که با توجه پوشش نسبتاً گسترده‌ی یک شبکه‌ی بی‌سیم که مانند شبکه‌های سیمی امکان محدودسازی دسترسی به صورت فیزیکی بسیار دشوار است. اطمینان از شانس پایین رخ دادن حملات نیز خود تضمینی ندارد.

11-6- Authentication با رمزنگاری RC4 (shared key Authentication)

این روش که به روش «کلید مشترک» نیز موسوم است، تکنیکی کلاسیک است که بر اساس آن، پس از اطمینان از اینکه مخدوم از کلیدی سری آگاه است، هویتش تأیید می‌شود. شکل 11-5 این روش را نشان می‌دهد.



شکل 5-11

در این روش، نقطه‌ی دسترسی (AP) یک رشته‌ی تصادفی تولید کرده و آن را به مخدوم می‌فرستد. مخدوم این رشته‌ی تصادفی را با کلیدی از پیش تعیین شده (که کلید WEP نیز نامیده می‌شود) رمز می‌کند و حاصل را برای نقطه‌ی دسترسی ارسال می‌کند. نقطه‌ی دسترسی به روش معکوس پیام دریافتی را رمزگشایی کرده و با رشته‌ی ارسال شده مقایسه می‌کند. در صورت هم‌سانی این دو پیام، نقطه‌ی دسترسی از اینکه مخدوم کلید صحیحی را در اختیار دارد اطمینان حاصل می‌کند. روش رمزنگاری و رمزگشایی در این تبادل روش RC4 است. در این میان با فرض اینکه رمزنگاری RC4 را روشی کاملاً مطمئن بدانیم، دو خطر در کمین این روش است.

الف) در این روش تنها نقطه‌ی دسترسی است که از هویت مخدوم اطمینان حاصل می‌کند. به بیان دیگر مخدوم هیچ دلیلی در اختیار ندارد که بداند نقطه‌ی دسترسی‌یی که با آن در حال تبادل داده‌های رمز است. نقطه‌ی دسترسی اصلی است.

ب) تمامی روش‌هایی که مانند این روش بر پایه‌ی سؤال و جواب بین دو طرف، با هدف احراز هویت یا تبادل اطلاعات حیاتی، قرار دارند با حملاتی تحت عنوان **man-in-the-middle** در خطر هستند. در این دسته از حملات نفوذگر میان دو طرف قرار می‌گیرد و به‌گونه‌یی هر یک از دو طرف را گمراه می‌کند.

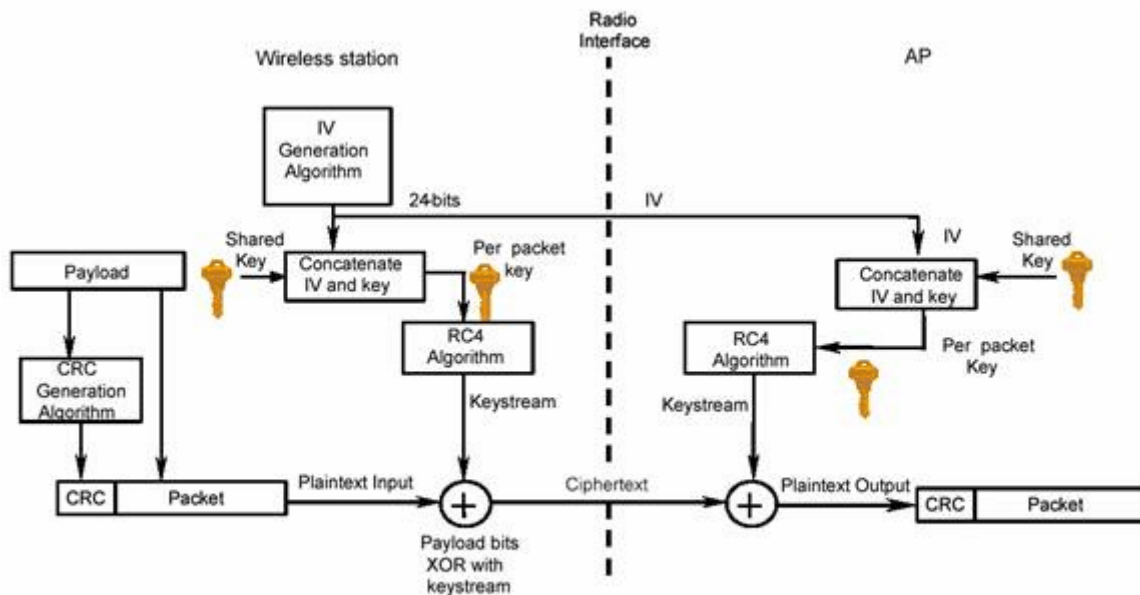
11-6-1- سرویس Privacy یا confidentiality

این سرویس که در حوزه‌های دیگر امنیتی اغلب به عنوان **Confidentiality** از آن یاد می‌گردد به معنای حفظ امنیت و محرمانه نگاه داشتن اطلاعات کاربر یا گره‌های در حال تبادل اطلاعات با یکدیگر است. برای رعایت محرمانه‌گی عموماً از تکنیک‌های رمزنگاری استفاده می‌گردد، به‌گونه‌یی که در صورت شنود اطلاعات در حال تبادل، این اطلاعات بدون داشتن کلیدهای رمز، قابل رمزگشایی نبوده و لذا برای شنودگر غیرقابل سوء استفاده است.

در استاندارد **802.11 b** از تکنیک‌های رمزنگاری **WEP** استفاده می‌گردد که برپایه **RC4** است. **RC4** یک الگوریتم رمزنگاری متقارن است که در آن یک رشته‌ی نیمه تصادفی تولید می‌گردد و توسط آن کل داده رمز می‌شود. این رمزنگاری بر روی تمام بسته‌ی اطلاعاتی پیاده می‌شود. به بیان دیگر داده‌های تمامی لایه‌های بالای اتصال بی‌سیم نیز توسط این روش رمز می‌گردند، از **IP** گرفته تا لایه‌های بالاتری مانند **HTTP**. از آنجایی که این روش عملاً اصلی‌ترین بخش از اعمال سیاست‌های امنیتی در شبکه‌های محلی بی‌سیم مبتنی بر استاندارد **802.11 b** است، معمولاً به کل پروسه‌ی امن‌سازی اطلاعات در این استاندارد به اختصار **WEP** گفته می‌شود.

کلیدهای **WEP** اندازه‌هایی از 40 بیت تا 104 بیت می‌توانند داشته باشند. این کلیدها با **IV** (مخفف **Initialization Vector** یا بردار اولیه) 24 بیتی ترکیب شده و یک کلید 128 بیتی **RC4** را تشکیل می‌دهند. طبیعتاً هرچه اندازه‌ی کلید بزرگ‌تر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان می‌دهد که استفاده از کلیدهایی با اندازه‌ی 80 بیت یا بالاتر عملاً استفاده از تکنیک **brute-force** را برای شکستن رمز غیرممکن می‌کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازه‌ی 80 بیت (که تعدد آن‌ها از مرتبه‌ی 24 است) به اندازه‌ی بالاست که قدرت پردازش سیستم‌های رایانه‌ی کنونی برای شکستن کلیدی مفروض در زمانی معقول کفایت نمی‌کند.

هرچند که در حال حاضر اکثر شبکه‌های محلی بی‌سیم از کلیدهای 40 بیتی برای رمزکردن بسته‌های اطلاعاتی استفاده می‌کنند ولی نکته‌ی که اخیراً بر اساس یک سری آزمایشات به دست آمده است، اینست که روش تأمین محرمانه‌گی توسط **WEP** در مقابل حملات دیگری، غیر از استفاده از روش **brute-force**، نیز آسیب‌پذیر است و این آسیب‌پذیری ارتباطی به اندازه‌ی کلید استفاده شده ندارد. نمایی از روش استفاده شده توسط **WEP** برای تضمین محرمانه‌گی در شکل 6-11 نمایش داده شده است.



شکل 6-11

Integrity -2-6-11

مقصود از Integrity صحت اطلاعات در حین تبادل است و سیاست‌های امنیتی‌یی که Integrity را تضمین می‌کنند روش‌هایی هستند که امکان تغییر اطلاعات در حین تبادل را به کم‌ترین میزان تقلیل می‌دهند. در استاندارد 2.11 b80 نیز سرویس و روشی استفاده می‌شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان مخدوم‌های بی‌سیم و نقاط دسترسی کم می‌شود. روش مورد نظر استفاده از یک کد CRC است. همان‌طور که در شکل قبل نیز نشان داده شده است، یک CRC-32 قبل از رمز شدن بسته تولید می‌شود. در سمت گیرنده، پس از رمزگشایی، CRC داده‌های رمزگشایی شده مجدداً محاسبه شده و با CRC نوشته شده در بسته مقایسه می‌گردد که هرگونه اختلاف میان دو CRC به معنای تغییر محتویات بسته در حین تبادل است. متأسفانه این روش نیز مانند روش رمزنگاری توسط RC4، مستقل از اندازه‌ی کلید امنیتی مورد استفاده، در مقابل برخی از حملات شناخته شده آسیب‌پذیر است.

متأسفانه استاندارد 802.11 b هیچ مکانیزمی برای مدیریت کلیدهای امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلیدها انجام می‌گیرد باید توسط کسانی که شبکه‌ی بی‌سیم را نصب می‌کنند به صورت دستی پیاده‌سازی گردد. از آنجایی که این بخش از امنیت یکی از معضله‌های اساسی در مبحث رمزنگاری است، با این ضعف عملاً روش‌های متعددی برای حمله به شبکه‌های بی‌سیم قابل تصور است. این روش‌ها معمولاً بر سهل‌انگاری‌های انجام‌شده از سوی کاربران و مدیران شبکه مانند تغییر ندادن کلید به صورت مداوم، لودادن کلید، استفاده از کلیدهای تکراری یا کلیدهای پیش فرض کارخانه و دیگر بی توجهی‌ها نتیجه‌ی جز درصد نسبتاً بالایی از حملات موفق به شبکه‌های بی‌سیم ندارد. این مشکل از شبکه‌های بزرگ‌تر بیش‌تر خود را نشان می‌دهد. حتا با فرض تلاش برای جلوگیری از رخداد چنین سهل‌انگاری‌هایی، زمانی که تعداد مخدوم‌های شبکه از حدی می‌گذرد عملاً کنترل کردن این تعداد بالا بسیار دشوار شده و گه‌گاه خطاهایی در گوشه و کنار این شبکه‌ی نسبتاً بزرگ رخ می‌دهد که همان باعث رخنه در کل شبکه می‌شود.

3-6-11- ضعف‌های اولیه‌ی امنیتی WEP

در این قسمت به بررسی ضعف‌های تکنیک‌های امنیتی پایه‌ی استفاده شده در این استاندارد می‌پردازیم. همان‌گونه که گفته شد، عملاً پایه‌ی امنیت در استاندارد 802,11 بر اساس پروتکل WEP استوار است. WEP در حالت استاندارد بر اساس کلیدهای 40 بیتی برای رمزنگاری توسط الگوریتم RC4 استفاده می‌شود، هرچند که برخی از تولیدکننده‌گان نگارش‌های خاصی از WEP را با کلیدهایی با تعداد بیت‌های بیش‌تر پیاده‌سازی کرده‌اند.

نکته‌یی که در این میان اهمیت دارد قائل شدن تمایز میان نسبت بالارفتن امنیت و اندازه‌ی کلیدهاست. با وجود آن که با بالارفتن اندازه‌ی کلید (تا 104 بیت) امنیت بالاتر می‌رود، ولی از آن‌جاکه این کلیدها توسط کاربران و بر اساس یک کلمه‌ی عبور تعیین می‌شود، تضمینی نیست که این اندازه تماماً استفاده شود. از سوی دیگر همان‌طور که در قسمت‌های پیشین نیز ذکر شد، دستیابی به این کلیدها فرایند چندان سختی نیست، که در آن صورت دیگر اندازه‌ی کلید اهمیت‌ی ندارد.

متخصصان امنیت بررسی های بسیاری را برای تعیین حفره های امنیتی این استاندارد انجام داده اند که در این راستا خطراتی که ناشی از حملاتی متنوع، شامل حملات غیرفعال و فعال است، تحلیل شده است. حاصل بررسی های انجام شده فهرستی از ضعف های اولیه ی این پروتکل است.

1. استفاده از کلیدهای ثابت WEP

2. Initialization Vector -IV

11-6-4- استفاده از کلیدهای ثابت WEP

یکی از ابتدایی ترین ضعف ها که عموماً در بسیاری از شبکه های محلی بی سیم وجود دارد استفاده از کلیدهای مشابه توسط کاربران برای مدت زمان نسبتاً زیاد است. این ضعف به دلیل نبود یک مکانیزم مدیریت کلید رخ می دهد. برای مثال اگر یک کامپیوتر کیفی یا جیبی که از یک کلید خاص استفاده می کند به سرقت برود یا برای مدت زمانی در دسترس نفوذگر باشد، کلید آن به راحتی لو رفته و با توجه به تشابه کلید میان بسیاری از ایستگاه های کاری عملاً استفاده از تمامی این ایستگاه ها ناامن است. از سوی دیگر با توجه به مشابه بودن کلید، در هر لحظه کانال های ارتباطی زیادی توسط یک حمله نفوذپذیر هستند.

11-6-5- Initialization Vector - IV

این بردار که یک فیلد 24 بیتی است در قسمت قبل معرفی شده است. این بردار به صورت متنی ساده فرستاده می شود. از آن جایی که کلیدی که برای رمزنگاری مورد استفاده قرار می گیرد بر اساس IV تولید می شود، محدوده ی IV عملاً نشان دهنده ی احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است. به عبارت دیگر در صورتی که IV کوتاه باشد در مدت زمان کمی می توان به کلیدهای مشابه دست یافت. این ضعف در شبکه های شلوغ به مشکلی حاد مبدل می شود. خصوصاً اگر از کارت شبکه ی استفاده شده مطمئن نباشیم. بسیاری از کارت های شبکه از IV های ثابت استفاده می کنند و بسیاری از کارت های شبکه ی یک تولید کننده ی واحد IV های مشابه دارند. این خطر به همراه ترافیک بالا در یک شبکه ی شلوغ احتمال تکرار IV در مدت زمانی کوتاه را بالاتر می برد و در نتیجه کافی ست نفوذگر در مدت زمانی معین به ثبت داده های رمز شده ی شبکه بپردازد و IV های بسته های اطلاعاتی را ذخیره کند. با ایجاد بانکی از IV های استفاده شده در یک شبکه ی شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت.

11-7- ضعف در الگوریتم

از آن جایی که IV در تمامی بسته های تکرار می شود و بر اساس آن کلید تولید می شود، نفوذگر می تواند با تحلیل و آنالیز تعداد نسبتاً زیادی از IV ها و بسته های رمز شده بر اساس کلید تولید شده بر مبنای آن IV، به کلید اصلی دست پیدا کند. این فرایند عملی زمان بر است ولی از آن جاکه احتمال موفقیت در آن وجود دارد لذا به عنوان وضعی برای این پروتکل محسوب می گردد.

11-7-1- استفاده از CRC رمز نشده

در پروتکل WEP، کد CRC رمز نمی شود. لذا بسته های تأییدی که از سوی نقاط دسترسی بی سیم به سوی گیرنده ارسال می شود بر اساس یک CRC رمز نشده ارسال می گردد و تنها در صورتی که نقطه ی دسترسی از صحت بسته اطمینان حاصل کند تأیید آن را می فرستد. این ضعف این امکان را فراهم می کند که نفوذگر برای رمزگشایی یک بسته، محتوای آن را تغییر دهد و CRC را نیز به دلیل این که رمز نشده است، به راحتی عوض کند و منتظر عکس العمل نقطه ی دسترسی بماند که آیا بسته ی تأیید را صادر می کند یا خیر. ضعف های بیان شده از مهم ترین ضعف های شبکه های بی سیم مبتنی بر پروتکل WEP هستند. نکته یی که در مورد ضعف های فوق باید به آن اشاره کرد این است که در میان این ضعف ها تنها یکی از آن ها (مشکل امنیتی سوم) به ضعف در الگوریتم رمزنگاری باز می گردد و لذا با تغییر الگوریتم رمزنگاری تنها این ضعف است که برطرف می گردد و بقیه ی مشکلات امنیتی کماکان به قوت خود باقی هستند. جدول 1-11 ضعف های امنیتی پروتکل WEP را به اختصار جمع بندی کرده است.

جدول 1-11

Security Issue / Vulnerability	Remarks
1. Security features in vendor products are frequently not enabled.	Security features, albeit poor in some cases, are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.
2. IVs are short (or static).	24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
3. Cryptographic keys are short.	40-bit keys are inadequate for any system. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a compromise is possible from a brute-force attack.
4. Cryptographic keys are shared.	Keys that are shared can compromise a system. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
5. Cryptographic keys cannot be updated automatically and frequently.	Cryptographic keys should be changed often to prevent brute-force attacks.
6. RC4 has a weak key schedule and is inappropriately used in WEP.	The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 keystream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries.
7. Packet integrity is poor.	CRC32 and other linear block codes are inadequate for providing cryptographic integrity. Message modification is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of noncryptographic protocols often facilitates attacks against the cryptography.
8. No user authentication occurs.	Only the device is authenticated. A device that is stolen can access the network.
9. Authentication is not enabled; only simple SSID identification occurs.	Identity-based systems are highly vulnerable particularly in a wireless system.
10. Device authentication is simple shared-key challenge-response.	One-way challenge-response authentication is subject to "man-in-the-middle" attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

11-7-2- ویژگی های سیگنال های طیف گسترده

عبارت طیف گسترده به هر تکنیکی اطلاق می شود 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 می شود 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 ویژگی های جالب توجه سیگنال های طیف گسترده نهفته است. این ویژگی های 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 می رسد. مصونیت بالا در مقابل پارازیت و تداخل

امکان استفاده در CDMA

مزایای فوق کمیسیون FCC را بر آن داشت که در سال 1985 مجوز استفاده از این سیگنال ها را با محدودیت حداکثر توان یک وات در محدوده ISM صادر نماید.

11-7-3- سیگنال های 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 می کند. در این شکل سیگنال اطلاعات با استفاده از یک تسهیم کننده دیجیتال و با استفاده از روش تسهیم FSK تلفیق می شود. فرکانس سیگنال حامل نیز به شکل شبه تصادفی از محدوده فرکانسی بزرگ تری در مقایسه با سیگنال اطلاعات انتخاب می شود. با توجه به اینکه فرکانس های **pn-code** با استفاده از یک ثبات انتقالی همراه با پس خور ساخته می شوند، لذا دنباله فرکانسی تولید شده توسط آن کاملاً تصادفی نیست و به همین خاطر به این دنباله، شبه تصادفی می گوئیم. بر اساسی مقررات FCC و سازمان های قانون گذاری، حداکثر زمان توقف در هر کانال فرکانسی 400 میلی ثانیه است که برابر با حداقل 2,5 جهش فرکانسی در هر ثانیه خواهد بود. در استاندارد 802,11 حداقل فرکانس جهش در آمریکای شمالی و اروپا 6 مگاهرتز و در ژاپن 5 مگاهرتز می باشد.

11-7-4- سیگنال های طیف گسترده با توالی مستقیم

اصل حاکم بر توالی مستقیم، پخش یک سیگنال بر روی یک باند فرکانسی بزرگتر از طریق تسهیم آن با یک امضاء یا کُد به گونه ای است که نویز و تداخل را به حداقل برساند. برای پخش کردن سیگنال هر بیت واحد با یک کُد تسهیم می شود. در گیرنده نیز سیگنال اولیه با استفاده از همان کد بازسازی می گردد. در استاندارد 802,11 روش مدولاسیون مورد استفاده در سیستم های DSSS روش تسهیم DPSK است. در این روش سیگنال اطلاعات به شکل تفاضلی تسهیم می شود. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد.

از آنجا که در استاندارد 802,11 و سیستم DSSS از روش تسهیم DPSK استفاده می شود، داده های خام به صورت تفاضلی تسهیم شده و ارسال می شوند و در گیرنده نیز یک آشکار ساز تفاضلی سیگنال های داده را دریافت می کند. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد. در روش تسهیم PSK فاز سیگنال حامل با توجه به الگوی بیتی سیگنال های داده تغییر می کند. به عنوان مثال در تکنیک QPSK دامنه سیگنال حامل ثابت است ولی فاز آن با توجه به بیت های داده تغییر می کند. جدول زیر ایده مدولاسیون فاز را نشان می دهد. در الگوی مدولاسیون QPSK چهار فاز مختلف مورد استفاده قرار می گیرند و چهار نماد را پدید می آورند. 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 می شوند. به عنوان مثال در روش $\pi/4$ -DQPSK، چهار مقدار تغییر فاز $3\pi/4$ ، $\pi/4$ ، $3\pi/4$ و $\pi/4$ است. با توجه به اینکه در روش فوق چهار تغییر فاز به کار رفته است لذا هر نماد می تواند دو بیت را کُدگذاری نماید.

جدول 2-11 مدولاسیون

اختلاف فاز	بینهای زوج	بینهای فرد
$3\pi/4$	۱	۱
$\pi/4$ ۳	۱	۰
$\pi/4$	۰	۰
$\pi/4$	۰	۱

در روش تسهیم طیف گسترده با توالی مستقیم مشابه تکنیک FH از یک کد شبه تصادفی برای پخش و گسترش سیگنال استفاده می شود. 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 می شود. در این تکنیک نرخ بیتی شبه کد تصادفی، نرخ تراشه نامیده می شود. در استاندارد 802,11 از کدی موسوم به کد بارکر برای تولید کدها تراشه سیستم DSSS استفاده می شود. مهم ترین 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.

استفاده مجدد از فرکانس

یکی از نکات مهم در طراحی شبکه های بی سیم، طراحی شبکه سلولی به گونه ای است که تداخل فرکانسی را تا جای ممکن کاهش دهد.

8-11 - مقایسه مدل های 802,11

802.11 b -1-8-11 استاندارد

همزمان با برپایی استاندارد IEEE 802.11b یا به اختصار 11.b در سال 1999، انجمن مهندسين برق و الكترونيك تحول قابل توجهی در شبکه سازی های رایج و مبتنی بر اترنت ارائه کرد. این استاندارد در زیر لایه دسترسی به رسانه از پروتکل CSMA/CA سود می برد. سه تکنیک رادیویی مورد استفاده در لایه فیزیکی این استاندارد به شرح زیر است.

- استفاده از تکنیک رادیویی **DSSS** در باند فرکانسی **2.4 GHz** به همراه روش مدولاسیون **CCK**
- استفاده از تکنیک رادیویی **FHSS** در باند فرکانسی **2.4 GHz** به همراه روش مدولاسیون **CCK**
- استفاده از امواج رادیویی مادون قرمز.

در استاندارد 802.11، اولیه نرخ‌های ارسال داده 1 و 2 مگابیت در ثانیه است. در حالی که در استاندارد **802.11 b** با استفاده از تکنیک **CCK** و روش تسهیم **QPSK** نرخ ارسال داده به 5.5 مگابیت در ثانیه افزایش می‌یابد همچنین با به کارگیری تکنیک **DSSS** نرخ ارسال داده به 11 مگابیت در ثانیه می‌رسد. به طور سنتی این استاندارد از دو فناوری **DSSS** یا **FHSS** استفاده می‌کند. هر دو روش فوق برای ارسال داده با نرخ های 1 و 2 مگابیت در ثانیه مفید هستند. جدول 3-11 سرعت مختلف قابل دسترسی در این استاندارد را نشان می‌دهد.

جدول 3-11 – نرخهای ارسال داده ها در استاندارد 802.11 b

Bits/Symbol	Symbol Rate	Modulation	Code Length	Data Rate
1	1 MSps	BPSK	11 (Barker Sequence)	1 Mbps
2	1 MSps	QPSK	11 (Barker Seq.)	2 Mbps
4	1.375 MSps	QPSK	8 CCK	5.5 Mbps
8	1.375 MSps	QPSK	8 CCK	11 Mbps

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 **2.4 GHz** تا **2.4835 GHz** برای فناوری‌های رادیویی استاندارد **IEEE 802.11b** اختصاص داده است.

11-8-1-1- اثرات فاصله

فاصله از فرستنده بر روی کارایی و گذردهی شبکه‌های بی سیم تاثیر قابل توجهی دارد. فواصل رایج در استاندارد 802.11 با توجه به نرخ ارسال داده تغییر می‌کند و به طور مشخص در پهنای باند **11Mbps** این فاصله 30 تا 45 متر و در پهنای باند 5.5 تا 45 متر و در پهنای باند 2 تا 107 متر است. لازم به یادآوری

است که این فواصل توسط عوامل دیگری نظیر کیفیت و توان سیگنال، محل استقرار فرستنده و گیرند و شرایط فیزیکی و محیطی تغییر می کنند.

در استاندارد **802.11 b** پروتکلی وجود دارد که گیرنده بسته را ملزم به ارسال بسته تصدیق می نماید. توجه داشته باشید که این مکانیزم تصدیق علاوه بر مکانیزم های تصدیق رایج در سطح لایه انتقال (نظیر آنچه در پروتکل **TCP** اتفاق می افتد) عمل می کند. در صورتی که بسته تصدیق ظرف مدت زمان مشخصی از طرف گیرنده به فرستنده نرسد، فرستنده فرض می کند که بسته از دست رفته است و مجدداً آن بسته را ارسال می کند. در صورتی که این وضعیت ادامه یابد نرخ ارسال داده نیز کاهش می یابد (**Fall Back**) تا در نهایت به مقدار **1Mbps** برسد. در صورتی که در این نرخ حداقل نیز فرستنده بسته های تصدیق را در زمان مناسب دریافت نکند ارتباط گیرنده را قطع شده تلقی کرده و دیگر بسته های را برای آن گیرنده ارسال نمی کند. به این ترتیب فاصله نقش مهمی در کارایی (میزان بهره وری از شبکه) و گذردهی (تعداد بسته های غیر تکراری ارسال شده در واحد زمان) ایفا می کند.

11-8-1-2- پل بین شبکه ای

بر خلاف انتظار بسیاری از کارشناسان شبکه های کامپیوتری، پل بین شبکه ای یا **Bridging** در استاندارد **802.11 b** پوشش داده نشده است. در پل بین شبکه ای 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 می شود. 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 می باشد. با وجود اینکه استاندارد **802.11 b** این کاربرد را پوشش نمی دهد ولی بسیاری از شرکت ها پیاده سازی های انحصاری از پل بی سیم را به صورت گسترش و توسعه استاندارد **802.11 b** ارائه کرده اند. پل های بی سیم نیز توسط مقررات **FCC** کنترل می شوند و گذردهی مؤثر یا به عبارت دیگر توان مؤثر ساطع شده همگرا (**EIRP**) در این تجهیزات نباید از 4 وات بیشتر باشد. بر اساس مقررات **FCC** توان سیگنال های ساطع شده در شبکه های محلی نیز نباید از 1 وات تجاوز نماید.

11-8-1-3- پدیده چند مسیری

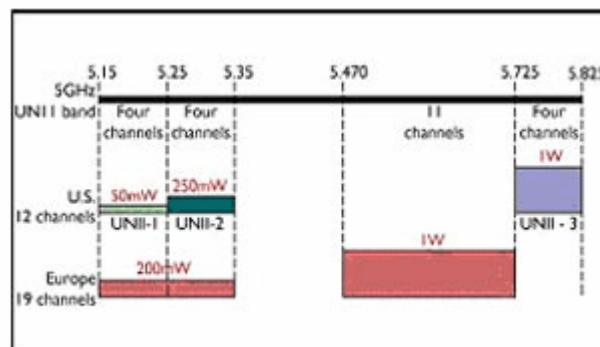
در این پدیده مسیر و زمان بندی سیگنال در اثر برخورد با موانع و انعکاس تغییر می کند. پیاده سازی های اولیه از استاندارد **802.11 b** از تکنیک **FHSS** در لایه فیزیکی استفاده می کردند. از ویژگی های قابل توجه این تکنیک مقاومت قابل توجه آن در برابر پدیده چند مسیری است. در این تکنیک از کانال های متعددی (79 کانال) با پهنای باند نسبتاً کوچک استفاده شده و فرستنده و گیرنده به تناوب کانال فرکانسی خود را تغییر می دهند. این تغییر کانال هر 400 میلی ثانیه بروز می کند لذا مشکل چند مسیری به شکل قابل ملاحظه ای منتفی می شود. زیرا گیرنده، سیگنال اصلی (که سریع تر از سایرین رسیده و عاری از تداخل است) را دریافت کرده و کانال فرکانسی خود را عوض می کند و سیگنال های انعکاسی زمانی به گیرنده می رسد که گیرنده کانال فرکانسی قبلی خود را عوض کرده و در نتیجه توسط گیرنده احساس و دریافت نمی شوند.

8-8-2- استاندارد 802.11 a

استاندارد 802.11 a، از باند رادیویی جدیدی برای شبکه های محلی بی سیم استفاده می کند و پهنای باند شبکه های بی سیم را تا 54Mbps افزایش می دهد. این افزایش قابل توجه در پهنای باند مدیون تکنیک مدولاسیونی موسوم به OFDM است. نرخ های ارسال داده در استاندارد IEEE 802.11a عبارتند از: 6،9،12،18،24،36،48،54 Mbps که بر اساس استاندارد، پشتیبانی از سرعت های 6،12،24 مگابیت در ثانیه اجباری است. برخی از کارشناسان شبکه های محلی بی سیم، استاندارد IEEE 802.11a را نسل آینده IEEE 802.11 تلقی می کنند و حتی برخی از محصولات مانند تراشه های Atheros و کارت های شبکه PCMCIA/Cardbus محصول Card Access Inc. استاندارد IEEE 802.11a را پیاده سازی کرده اند. بدون شک این پهنای باند وسیع و نرخ داده سریع محدودیت هایی را نیز به همراه دارد. در واقع افزایش پهنای باند در استاندارد IEEE 802.11a باعث شده است که محدوده عملیاتی آن در مقایسه با IEEE 802.11 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 قیمت زیرساختار شبکه بی سیم می شود. زیرا محدوده عملیاتی در این استاندارد کمتر از محدوده عملیاتی در استاندارد IEEE 802.11b 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 می کند. این باند فرکانسی به سه قطعه پیوسته فرکانسی به شرح زیر تقسیم می شود.

UNII-1 @ 5.2 GHz
 UNII-2 @ 5.7 GHz
 UNII-3 @ 5.8 GHz

یکی از تصورات غلط در زمینه استانداردهای 802.11 این باور است که 802.11 a قبل از 802.11 b مورد بهره برداری واقع شده است. در حقیقت 802.11 b نسل دوم استانداردهای بی سیم (پس از 802.11) است و 802.11 a نسل سوم از این مجموعه استاندارد به شمار می رود. استاندارد 802.11 a برخلاف ادعای بسیاری از فروشندگان تجهیزات بی سیم نمی تواند جایگزین 802.11 b شود زیرا لایه فیزیکی مورد استفاده در هر یک تفاوت اساسی با دیگری دارد. از سوی دیگر گذردهی (نرخ ارسال داده) و فواصل در هر یک متفاوت است.



شکل 7-11 - تخصیص باند فرکانسی در unii

در شکل 7-11 این سه ناحیه عملیاتی UNII و نیز توان مجاز تشعشع رادیویی از سوی FCC ملاحظه می شود. این سه ناحیه کاری 12 کانال فرکانسی را فراهم می کنند. باند UNII-1 برای کاربردهای فضای بسته، باند UNII-2 برای کاربردهای فضای بسته و باز و باند UNII-3 برای کاربردهای فضای باز و پل بین شبکه‌ای به کار برده می شوند. این نواحی فرکانسی در ژاپن نیز قابل استفاده هستند. این استاندارد در حال حاضر در قاره اروپا قابل استفاده نیست. در اروپا HyperLAN2 برای شبکه‌های بی سیم مورد استفاده قرار می گیرد که به طور مشابه از باند فرکانسی 802.11 a استفاده می کند. یکی از نکات جالب توجه در استاندارد 802.11 a 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 می نماید. در یکی تقسیم بندی کلی می توان ویژگی ها و مزایای 802.11 a را در سه محور زیر خلاصه نمود.

- افزایش در پهنای باند در مقایسه با استاندارد 802.11 b (در استاندارد 802.11 a حداکثر پهنای باند 54Mbps
- استفاده از طیف فرکانسی خلوت (باند فرکانسی 5GHz)
- استفاده از 12 کانال فرکانسی غیرپوشا (سه محدود هفرکانسی که در هر یک 4 کانال غیرپوشا وجود دارد)

8-11-2-1- افزایش پهنای باند

استاندارد 802.11 a در مقایسه با 802.11 b و پهنای باند 11 Mbps حداکثر پهنای باند 54 Mbps را فراهم می کند. مهم ترین عامل افزایش قابل توجه پهنای باند در این استاندارد استفاده از تکنیک پیشرفته مدولاسیون، موسوم به OFDM است. تکنیک OFDM یک تکنولوژی (فناوری) تکامل یافته و بالغ در کاربردهای بی سیم به شمار می رود. این تکنولوژی مقاومت قابل توجهی در برابر تداخل رادیویی داشته و تأثیر کمتری از پدیده چند مسیری می پذیرد. OFDM تحت عنوان مدولاسیون چند حاملی و یا مدولاسیون چند آهنگی گسسته نیز شناخته می شود. این تکنیک مدولاسیون علاوه بر شبکه‌های بی سیم در تلویزیون های دیجیتال (در اروپا، ژاپن، و استرالیا) و نیز به عنوان تکنولوژی پایه در خطوط مخابراتی ADSL مورد استفاده قرار می گیرد. آندرو مک کورمیک Andrew McCormik از دانشگاه ادینبورو نمایش محاوره‌ای جالبی از این فناوری گردآوری کرده که در نشانی <http://www.ee.ed.ac.uk/~acmc/OFDMTut.html> قابل مشاهده است.

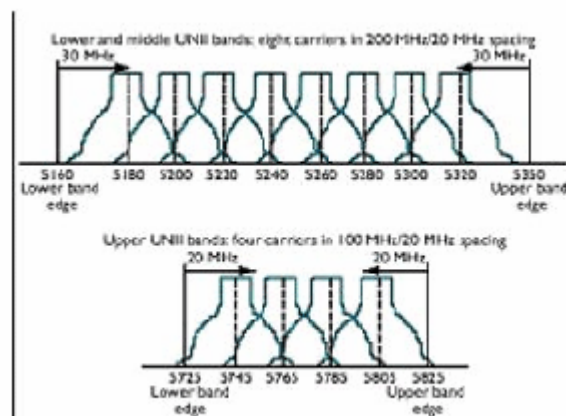
تکنیک OFDM از روش QAM و پردازش سیگنال های دیجیتال استفاده کرده و سیگنال داده را با فرکانس های دقیق و مشخصی تسهیم می کند. این فرکانس ها به گونه ای انتخاب می شوند که خاصیت تعامد را فراهم کنند و به این ترتیب علیرغم همپوشانی فرکانسی هر یک از فرکانس های حامل به تنهایی آشکار می شوند و نیازی به باند محافظت برای فاصله گذاری بین فرکانس ها نیست. برای کسب اطلاعات بیشتر در خصوص این تکنیک می توانید به نشانی زیر مراجعه نمایید.

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

در کنار افزایش پهنای باند در این استاندارد فواصل مورد استفاده نیز کاهش می یابند. در واقع باند فرکانسی **5 GHz** تقریباً دوبرابر باند فرکانسی است که در استاندارد **802.11 b** مورد استفاده قرار می گیرد. محدوده موثر در این استاندارد با توجه به سازندگان تراشه های بی سیم متفاوت و متغیر است ولی به عنوان یک قاعده سراسر می توان فواصل در این استاندارد را یک سوم محدوده فرکانسی **2.4GHz (802.11 b)** در نظر گرفت. در حال حاضر محدوده عملیاتی (فاصله از فرستنده) در محصولات مبتنی بر **802.11 a** و پهنای باند **54 Mbps** در حدود **10 تا 15 متر** است. این محدوده در پهنای باند **6Mbps** در حدود **61 تا 84 متر** افزایش می یابد.

8-11-2-2- طیف فرکانسی تمیزتر

طیف فرکانسی **UNII** در مقایسه با طیف **ISM** خلوت تر است و کاربرد دیگری برای طیف **UNII** به جز شبکه های بی سیم تعریف و تخصیص داده نشده است. در حالی که در طیف فرکانسی **ISM** تجهیزات بی سیم متعددی نظیر تجهیزات پزشکی، اجاق های مایکروویو، تلفن های بی سیم و نظایر آن وجود دارند. این تجهیزات بی سیم در باند **2.4GHz** یا طیف **ISM** هیچگونه تداخلی با تجهیزات باند **UNII** (تجهیزات بی سیم **802.11 a**) ندارند. شکل **8-11** فرکانس مرکزی و فاصله های فرکانسی در باند **UNII** را نشان می دهد.



شکل 8-11- فرکانس مرکزی و فواصل فرکانسی در باند **unii**

8-11-2-3- کانال های غیر پوشا

باند فرکانسی **UNII**، دوازده کانال منفرد و غیر پوشای فرکانسی را برای شبکه سازی فراهم می کند. از این **12** کانال **8** کانال مشخص (**UNII-1** , **2**) در شبکه های محلی بی سیم مورد استفاده قرار می گیرند. این ویژگی غیرپوشایی گسترش و پیاده سازی شبکه های بی سیم را ساده تر از باند **ISM** می کند که در آن تنها **3** کانال غیر پوشا از مجموع **11** کانال وجود دارد.

8-11-2-4- همکاری Wi-Fi

ائتلاف "همکاری اترنت بی سیم" یا <http://www.wi-fi.org> (WECA) کنسرسیومی از شرکت های Cisco, 3Com, Enterasys, Lucent و سایر شرکت های شبکه سازی است. اعضاء WECA از طریق همکاری مشترک تلاش دارند تا قابلیت همکاری تجهیزات بی سیم با یکدیگر را تضمین نمایند. برنامه گواهینامه Wi-Fi که توسط این گروه مطرح شده است نقش کلیدی در گسترش و پذیرش استاندارد IEEE 802.11 ایفا می کند. در حال حاضر این ائتلاف برای بیش از 100 محصول گواهی سازگاری Wi-Fi صادر کرده است و تعداد این محصولات رو به افزایش است. با گسترش فزاینده محصولات IEEE 802.11a, WECA برنامه دیگری برای صدور گواهینامه برای این نوع محصولات نیز ارائه می کند.

IEEE 802.11g-3-8-11 استاندارد بعدی

این استاندارد مشابه IEEE 802.11b از باند فرکانسی 2.4GHz (یا طیف ISM) استفاده می کند و از تکنیک OFDM به عنوان روش مدولاسیون بهره می برد. البته PBCC نیز یکی از روش های جایگزین و تحت بررسی برای انتخاب تکنیک مدولاسیون در این استاندارد به شمار می رود. IEEE 802.11g از نظر فرکانسی، تعداد کانال های غیرپوشا، و توان مشابه IEEE 802.11b است. محدوده های عملیاتی نیز کم و بیش مشابه هستند با این تفاوت که حساسیت OFDM به نویز تاحدودی این محدوده عملیاتی را کاهش می دهد. پهنای باند 54Mbps یکی از اهداف احتمالی این استاندارد جدید به شمار می رود. یکی دیگر از مزایای جالب توجه IEEE 802.11g سازگاری با IEEE 802.11b است. در نتیجه ارتقاء از تجهیزات IEEE 802.11b به استاندارد جدید IEEE 802.11g امری سراسر خواهد بود. جدول 4-11 سه استاندارد شبکه های بی سیم را با یکدیگر مقایسه می کند.

جدول 4-11 - مقایسه استانداردهای بی سیم IEEE 802.11

IEEE 802.11g	IEEE 802.11a	IEEE 802.11b	
<p>- ارتقاء شبکه های 802.11b و رقیبی برای 802.11a</p> <p>- کارایی مشابه با 802.11a در فواصل طولانی</p>	<p>- جایگزین شبکه های سیمی</p> <p>- فراهم کننده پهنای باند زیاد در کاربردهای (صدا، تصویر، CAD و نظایر آن)</p> <p>- شبکه سازی در محل هایی که استفاده از سیم میسر نیست.</p>	<p>- جایگزین شبکه های سیمی</p> <p>- فراهم آوردن تحرک و سیار بودن کاربران</p> <p>- شبکه سازی در محل هایی که استفاده از سیم میسر نیست</p> <p>- پل سازی بین شبکه های محلی در فواصل دور (40 کیلومتر)</p>	کاربردهای احتمالی
<p>- سازگاری با 802.11b</p> <p>- محدوده عملیاتی زیاد (نظیر 802.11b)</p> <p>- گذردهی (نرخ ارسال داده) بیشتر</p>	<p>- گذردهی (نرخ ارسال داده) بالا در فواصل کم</p> <p>- افزایش تعداد کانال های فرکانسی غیرپوشا (2 برابر بیشتر از 802.11b)</p> <p>- تداخل فرکانسی کمتر</p>	<p>- استاندارد رایج و تکامل یافته</p> <p>- قیمت منطقی</p> <p>- گذردهی قابل قبول در فاصله زیاد (نرخ ارسال داده)</p>	مزایا
<p>- عدم وجود محصول فراگیر (احتمالاً تا اواسط سال 2002 میلادی)</p> <p>- محدودیت ها کانال فرکانسی نظیر 3 (802.11b کانال غیرپوشا)</p>	<p>- فناوری نسبتاً گران</p> <p>- ناسازگاری با 802.11b</p> <p>- محدوده عملیاتی کوچک</p> <p>- محدودیت های FCC بر روی آنتن ها (حداکثر توان مجاز) در هر باند فرکانسی</p>	<p>- دارابودن کمترین گذردهی (نرخ ارسال داده) در مقایسه با سایر فناوری های بی سیم (11 Mbps)</p> <p>- استفاده از تنها 2 کانال فرکانسی غیر پوشا</p>	معایب

منابع

[1] ملکیان ، احسان ، 1384. اصول مهندسی اینترنت ، انتشارات نص.

[2] فایند، یونس، 1384. شبکه های wireless، انتشارات ادبستان.

[3] pc network

[4] <http://wireless.per.nl/telelearn/ofdm>

[5] <http://www.ee.ed.ac.uk/~acmc/OFDMTut.html>

[6] <http://ce.sharif.edu/~veisi/Education/Courses/ComputerNetworks/Presentations/Wireless.ppt>

[7] <http://database.irandoc.ac.ir/fulltext/TH/f.htm?26879>

[8] <http://database.irandoc.ac.ir/scripts/wxis.exe/?IsisScript=/iranint/scripts>

[9] <http://www.kcspot.net/upload/files/toto/Bluetooth.doc>

[10] [http:// www.echostar.com](http://www.echostar.com)