شبکه‌های بی‌سیم Wi-Fi

Wireless Fidelity

تهیه و تنظیم:

مهندس مجید عمرانی

WIRELESS FIDELITY

- شبکه‌های بی‌سیم، بسیار شبیه شبکه‌های باسیم هستند. تفاوت اصلی این دو شبکه این است که برخلاف شبکه‌های باسیم، در شبکه‌های وایرلس، دستگاه‌ها برای اتصال به روتر از کابل (سیم) استفاده نمی‌کنند. درواقع به جای کابل، از ارتباط بی‌سیم استفاده می‌کنند که تحت عنوان وای‌فای (Wireless Fidelity) شناخته می‌شود Wi-Fi. نام دیگر استاندارد شبکه ۸۰۲.۱۱ است. استانداردی که توسط انستیتو مهندسان برق و الکترونیک (IEEE) پشتیبانی می‌شود. با توجه به این مسأله، دستگاه‌های وایرلس، نیازی به پورت نداشته و تنها کافی است مجهز به آنتن باشند. این آنتن در مواردی درون دستگاه، مخفی شده است.

- به طور معمول، در شبکه‌های خانگی هر دو دستگاه باسیم و بی‌سیم وجود داشته و با یکدیگر در ارتباط هستند؛ از این رو ممکن است به Access Point یا Wi-Fi Client نیاز داشته باشند.

- اکسس‌پوینت یک دستگاه مرکزی است که سیگنال‌های وای‌فای را برای کلاینت‌های شبکه ارسال می‌کند. به طور کلی هر شبکه‌ای وایرلسی که شما هنگام قدم زدن در خیابان یا ایستادن در امکان عمومی یا فرودگاه‌ها بر روی تلفن‌همراه خود مشاهده می‌کنید از یک اکسس‌پوینت برای شما ارسال شده

- شما می‌توانید با خرید یک اکسس‌پوینت مجزا و اتصال آن به روتر یا سوئیچ، سیگنال وای‌فای را در شبکه خود فراهم کنید. اما معمولاً بهتر است یک روتر وایرلس (که یک پورت WAN و یک پورت LAN دارد) مجهز به یک اکسس‌پوینت داخلی خریداری کرد. بعضی از روترها هم با دو اکسس‌پوینت داخلی (Dual-Band Router) عرضه می‌شوند.
  امروزه بسیاری از مودم های ADSL یا وای-ماکس دارای اکسس‌پوینت داخلی هستند و اینترنت را به صورت بی سیم در اختیار کاربر قرار می‌دهند .

- یک Wi-Fi Client یاWLAN Client ، وسیله‌ای است که می‌تواند سیگنال‌های منتشر شده به وسیله اکسس‌پوینت را شناسایی کرده و به شبکه آن متصل شود.

- اکثر لپ‌تاپ‌ها، تلفن‌های هوشمند و تبلت با وای‌فای و اتصال به شبکه‌های بی‌سیم سازگار هستند. آن دسته از وسایلی که سازگار نیستند هم می‌توانند به کمک کارت‌های وای‌فای USB یا

آداپتورهای PCIe وای‌فای به شبکه‌های بی‌سیم متصل شوند. برای راحتی می‌توان اینگونه تصور کرد که Wi-Fi Client ها، پورت و کابل شبکه نامرئی برای اتصال به شبکه دارند !

برد وای‌فای(Wi-Fi Range)

- برد سیگنال‌های وای‌فای، شعاع انتشار سیگنال‌های منتشر شده توسط اکسس‌پوینت است. معمولاً سیگنال‌های وای‌فای تا فاصله ۴۵ متری از اکسس‌پوینت مؤثر و کاربردی محسوب می‌شوند. البته این فاصله با توجه به قدرت دستگاه‌های درگیر در شبکه، شرایط محیطی و علی‌الخصوص استاندارد امواج وای‌فای متغییر است.

- یک اکسس‌پوینت ایده‌آل و قدرتمند، قادر است سیگنال‌های وای‌فای را تا شعاع ۹۰ متری یا حتی بیشتر منتشر کند.

- استاندارد امواج (سیگنال‌های) وای‌فای، تعیین‌کننده سرعت یک ارتباط بی‌سیم نیز هست. به همین دلیل، کار با وای‌فای و پیکربندی شبکه‌های مبتنی بر آن، در مواقعی پیچیده و گیج‌کننده می‌شود.

- برد سیگنال‌های وای‌فای، شعاع انتشار سیگنال‌های منتشر شده توسط اکسس‌پوینت است. معمولاً سیگنال‌های وای‌فای تا فاصله ۴۵ متری از اکسس‌پوینت مؤثر و کاربردی محسوب می‌شوند. البته این فاصله با توجه به قدرت دستگاه‌های درگیر در شبکه، شرایط محیطی و علی‌الخصوص استاندارد امواج وای‌فای متغییر است.
- یک اکسس‌پوینت ایده‌آل و قدرتمند، قادر است سیگنال‌های وای‌فای را تا شعاع ۹۰ متری یا حتی بیشتر منتشر کند.
- استاندارد امواج (سیگنال‌های) وای‌فای، تعیین‌کننده سرعت یک ارتباط بی‌سیم نیز هست. به همین دلیل، کار با وای‌فای و پیکربندی شبکه‌های مبتنی بر آن، در مواقعی پیچیده و گیج‌کننده می‌شود.

- باندها در حقیقت سیگنال‌های رادیویی هستند که توسط استانداردهای وای‌فای مورد استفاده قرار می‌گیرند. فرکانس این سیگنال‌ها عبارتند از ۲,۴ گیگاهرتز، ۵ گیگاهرتز و ۶۰ گیگاهرتز.

- ۲,۴ گیگاهرتز، در حال حاضر محبوب‌ترین و متداول‌ترین فرکانس وای‌فای است. به این معنا که توسط اکثر دستگاه(Wi-Fi Client) ها مورد استفاده قرار می‌گیرد. علاوه بر وای‌فای کلاینت‌ها، دستگاه الکترونیکی دیگری مانند تلفن‌های بی‌سیم نیز از این فرکانس استفاده می‌کنند.

- همانگونه که می‌توان حدس زد، کیفیت این فرکانس کمتر از فرکانس ۵ گیگاهرتز است.

- بسته به استاندارد وای‌فای، بعضی از دستگاه‌ها، از یک یا هر دو استاندارد ۲,۴ و ۵ گیگاهرتزی پشتیبانی می‌کنند. البته دستگاه‌هایی نیز وجود دارند که از هر سه استاندارد پشتیبانی کرده و دستگاه‌های Tri-Band نامیده می‌شوند. با توجه به این تعریف، دستگاه‌هایی که از دو استاندارد پشتیبانی می‌کنند، Dual-Bandنامیده می‌شوند.

استانداردهای وای‌فای

- **802.11b**

این نمونه، اولین استاندارد وایرلس تجاری محسوب می‌شود که در سال ۱۹۹۹ عرضه شد. بالاترین سرعت تبادل اطلاعات در این استاندارد، ۱۱ مگابیت در ثانیه است و تنها از فرکانس ۲,۴ گیگاهرتز استفاده می‌کند. این استاندارد همچنان توسط اکسس‌پوینت و روترهای جدید پشتیبانی می‌شود.

- **802.11a**

این استاندارد، مشابه نمونه قبلی است، با این تفاوت حداکثر سرعت ۵۴ مگابیت در ثانیه را برای کاربر فراهم کرده و از فرکانس ۵ گیگاهرتز استفاده می‌کند. این استاندارد هم همچنان توسط اکثر اکسس‌پوینت و روترهای جدیدتر پشتیبانی می‌شود .

- **802.11g**

این استاندارد، سال ۲۰۰۳ معرفی شد. در استاندارد 802.11 gبرای اولین بار شبکه‌های وایرلس «وای‌فای» نامیده شدند. این استاندارد که حداکثر سرعت ۵۴ مگابیت در ثانیه را فراهم نموده، از فرکانس ۲,۴ گیگاهرتز بهره می‌برد. تفاوت این استاندارد با استاندارد قبلی در برد بیشتر سیگنال‌های آن است. این استاندارد همچنان در بعضی تلفن‌های هوشمند مانند آیفون 3 Gو آیفون 3 GSو اکسس‌پوینت‌های جدیدتر پشتیبانی می‌شود.

- **802.11nیاWireless-N**

این استاندارد از سال ۲۰۰۹ در دسترس کاربران قرار گرفت و در حال حاضر، متداول‌ترین استاندارد وای‌فای محسوب می‌شود. این استاندارد، درواقع نسخه‌ای اصلاح‌شده و بهبود یافته از

استانداردهای پیشین است. بهبودهای این استاندارد در موارد مختلفی مانند برد (Range) سیگنال‌ها، پشتیبانی از دو فرکانس ۲,۴ و ۵ گیگاهرتزی بود. این استاندارد، زمینه را برای ظهور روترهای Dual-Band فراهم نمود، دستگاه‌هایی که بر روی هر دو فرکانس استاندارد-Wireless Nبه خوبی کار می‌کردند.

- **استانداردWireless-N ، بر روی هر یک از فرکانس‌های اشاره شده، در سه سطح-single stream و dual-stream و three-stream در دسترس است که به ترتیب سرعت ۱۵۰، ۳۰۰ و ۴۵۰ مگابیت در ثانیه را فراهم می‌کند. این استاندارد منجر به تولید سه نوع روتر Dual-Bandشد:**
- **-روترهای : N600 پشتیبانی از هر دو فرکانس و ارائه سرعت ۳۰۰ مگابیت در ثانیه**
- **-روترهای : N750 ارائه سرعت ۳۰۰ مگابیت در ثانیه برای یکی از فرکانس‌ها و سرعت ۴۵۰ مگابیت در ثانیه برای فرکانس دیگر**
- **-روترهای : N900 پیشتیبانی از هر دو فرکانس با سرعت ۴۵۰ مگابیت در ثانیه**

(وای‌فای نسل پنجم) 5G Wi-Fi یا ۸۰۲.۱۱AC

- آخرین استاندارد وای‌فای تنها از فرکانس ۵ گیگاهرتز استفاده کرده و در حال Three-Stream، سرعت انتقالی نزدیک به ۱.۳ گیگابیت در ثانیه را فراهم می‌کند. این نسل، از تنظیمات Double-Stream و Single-Stream نیز پشتیبانی می‌کند که به ترتیب با سرعت ۹۰۰ و ۴۵۰ مگابیت در ثانیه سازگار هستند.
- *توضیح: سرعت حالت Single-Stream در استاندارد ۸۰۲.۱۱ac، با سرعت Three-Stream در استاندارد ۸۰۲.۱۱n برابر است.*
- در حال حاضر، تعداد محدودی روتر سازگار با استاندارد ۸۰۲.۱۱ ac در بازار وجود دارد. اما با ورود تبلت‌ها و تلفن‌های هوشمندی که روتر داخلی سازگار با این استاندارد دارند، آینده این استاندارد درخشان‌تر خواهد شد.

- **از نظر فنی، استاندارد 802.11 ac سه برابر سریعتر از استاندارد 802.11 n است. و به همین دلیل انرژی کمتر برای دریافت اطلاعات مصرف می‌کنند و در نتیجه با باتری دستگاه‌های همراه ملایم‌تر برخورد می‌کند! اما در عمل چون سرعت انتقال از سرعت تئوریک محیط آزمایشگاهی کمتر است، 802.11 ac دو برابر سریعتر از استاندارد Wireless-N است.**

WiGig یا ۸۰۲.۱۱ad

- این استاندارد، در زمان برگزاری نمایشگاه CES ۲۰۱۳ به اکوسیستم وای‌فای وارد شد. پیش از این زمان، WiGigرا به عنوان نوع متفاوتی از شبکه بی‌سیم می‌شناختند.
- ۸۰۲.۱۱adاز فرکانس ۶۰ گیگاهرتز استفاده می‌کند که منجر به ارائه سرعتی در حدود ۷ گیگابیت در ثانیه (یعنی هفت برابر سریعتر از یک اتصال Gigabit Ethernet)می‌شود.
- اما در مقایسه با سایر استانداردها، از بردی کوتاه‌تر (در حدود ۹ متر) برخوردار است. به همین دلیل این استاندارد برای پوشش‌های محیطی و دستگاه‌های جانبی نزدیک، مثل لپ‌تاپ‌ها یا ایستگاه‌های تبلیغاتی مناسب‌تر است.
- پس از CES ۲۰۱۳ ، روز به روز به تعداد دستگاه‌های پشتیبان کننده از این استاندارد افزوده می‌شود. البته پیشتیانی از این استاندارد در دستگاه‌های مختلف در کنار استانداردهای دیگر انجام می‌شود.

تهدیدهای امنیتی

- هنگامی که سیگنال وای‌فای از طریق اکسس‌پوینت ارسال (Broadcast) می‌شوند، واقعاً همه چیز روی هوا است! هر شخصی که مجهز به یک کلاینت وای‌فای باشد، می‌تواند به این اکسس‌پوینت متصل شود. این خاصیت، ممکن است منجر به بروز تهدیدهای امنیتی زیادی بشود. برای جلوگیری از وقوع اینگونه اتفاقات، شبکه‌های وای‌فای معمولاً به کمک کلمه‌عبور (و در شرایط حیاتی‌تر به کمک کلمه‌عبور رمزنگاری شده) از اتصال‌های غیرمجاز جلوگیری می‌کنند. در حال حاضر متدهای مختلفی برای محافظت از شبکه‌های وای‌فای وجود دارد که به آن‌ها متدهای تصدیق هویت (Authentication Methods) گفته می‌شود WPA . ، WEPو WPA ۲ از جمله این متدها هستند.

- **WEP=Wired Equivalent Privacy**

در اين روش از شنود كاربرهايي كه در شبكه مجوز ندارند جلوگيري به عمل مي آيد كه مناسب براي شبكه هاي كوچك بوده زيرا نياز به تنظيمات دستي(KEY) مربوطه در هر Clientمي باشد.
اساس رمز نگاري WEPبر مبناي الگوريتم RC4بوسيله RSAمي باشد.

- **SSID = Service Set Identifier**

شبكه هاي WLANداراي چندين شبكه محلي مي باشند كه هر كدام آنها داراي يك شناسه (Identifier)يكتا مي باشند اين شناسه ها در چندين Access Pointقرار داده مي شوند . هر كاربر براي دسترسي به شبكه مورد نظر بايستي تنظيمات شناسه SSIDمربوطه را انجام دهد .

- **MAC = Media Access Control**

ليستي از MACآدرس هاي مورد استفاده در يك شبكه به AP (Access Point) مربوطه وارد شده بنابراين تنها كامپيوترهاي داراي اين MACآدرسها اجازه دسترسي دارند به عبارتي وقتي يك كامپيوتر درخواستي را ارسال مي كند MACآدرس آن با ليست MACآدرس مربوطه در APمقايسه شده و اجازه دسترسي يا عدم دسترسي آن مورد بررسي قرار مي گيرد .اين روش امنيتي مناسب براي شبكه هاي كوچك بوده زيرا در شبكه هاي بزرگ امكان ورود اين آدرسها به APبسيار مشكل مي باشد.

تهدیدهای امنیتی

- متد ۲ WPA مانندWPA ، از **پروتکل تصدیق به کمک کلید موقت (TKIP)** و **استاندارد رمزنگاری پیشرفته (AES)** برای رمزنگاری سیگنال‌ها استفاده می‌کند. از TKIP برای اتصال کلاینت‌های قدیمی‌تر و AES که سرعت و امنیت بیشتری را فراهم می‌کند تنها برای اتصال دستگاه‌های جدیدتر قابل استفاده است.
- پس با تعریف یک کلمه‌عبور یا کلید رمزنگاری شده در یک اکسس‌پوینت، به کلاینت مجاز اجازه دسترسی داده خواهد شد.

WPS یا WiFi Protected Setup

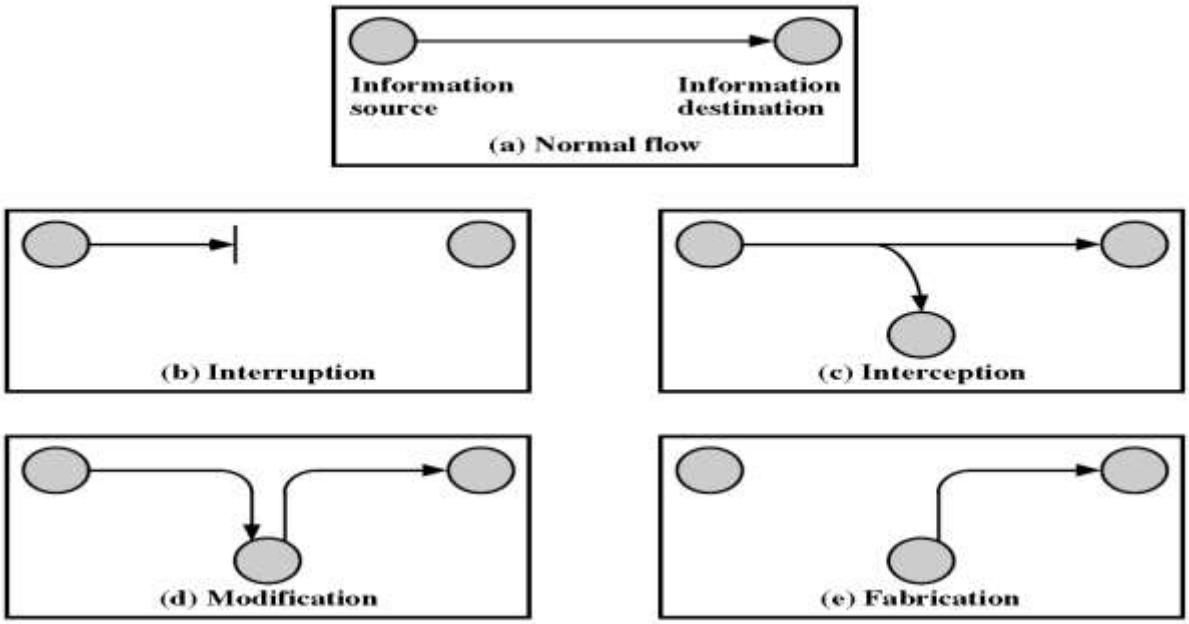
- این استاندارد که در سال ۲۰۰۷ معرفی شده است، راه‌اندازی یک شبکه ایمن را آسانتر می‌کند. تنها کاری که برای استفاده از این متد باید انجام داد، فشردن کلید WPS است.
- ابتدا باید بر روی اکسس‌پوینت، کلید WPS را فعال کنید و سپس در زمانی کمتر از ۲ دقیقه بر روی کلید WPS کلاینت بزنید تا به اکسس‌پوینت متصل شود. به کمک WPS نیازی به حفظ کردن پسورد ندارید. به خاطر داشته باشید که این ویژگی تنها در دستگاه‌های سازگار با این استاندارد قابل استفاده است. البته اغلب دستگاه‌های سال‌های گذشته از این استاندارد پشتیبانی می‌کنند.

- **حمله (Attack)**
  - **تلاش عمدی برای رخنه در یک سیستم یا سوء استفاده از آن**
- **رخنه (Breach)**
  - **نقض سیاست امنیتی یک سیستم (بایدها و نبایدها)**
- **نفوذ (Intrusion)**
  - **فرایند حمله و رخنه ناشی از آن**
- **آسیب پذیری (Vulnerability)**
  - **هرگونه نقطه ضعف که بتوان از آن سوء استفاده کرده و سیاست امنیتی را نقض کرد**
  - **نقطه ضعف در توصیف، طراحی، پیاده سازی، پیکربندی و اجرا**

- **Hack**
  - **کنکاش به منظور کشف حقایق و نحوه کار سیستم**
- **Attack**
  - **تلاش برای نفوذ به سیستم دیگران**
  - **هک خصمانه!**

Malicious Hacker = Attacker

- **حمله امنیتی (Security Attack)**
  - **عملی که امنیت اطلاعات سازمان را نقض کند**
- **سیاست امنیتی(Security Policy)**
  - **تعیین می کند که از جنبه امنیتی چه کارهایی مجاز یا غیر مجازند**
- **مکانیزم امنیتی(Security Mechanism)**
  - **روشی برای تشخیص، جلوگیری و بازیابی حملات**
  - **درواقع یکی از روشهای پیاده سازی یک سیاست امنیتی**
- **سرویس امنیتی(Security Service)**
  - **سرویسهای تضمین کننده با استفاده از مکانیزمهای امنیتی**



الگوهای حمله های متداول به شبکه های بی سیم

◄ الگوهای حملات غیرفعال

در این حملات، کاربر غیرمجاز به منـابع شبکه دسترسی پیدا می‌کند،اما نمی‌خواهد که متن پیامی را تغییر دهد، بلکه می‌خواهد از اطلاعات شبکه استفاده نماید.سه نوع حمله غیرفعال وجود دارد که عبارتند از:

۱- **پاسخ‌گویی:** در این روش، هکر به کانال داده‌ها دسترسی دارد و در ابتدای کار زیانی به سیستم وارد نمی‌کند،اما می‌تواند بعضی پیام‌ها را طوری به کـــاربران مجـــاز شبکه بفرستد که آن‌ها گمان کنند پیام از جانب سرور آمده است.

۲- **Eavesdropping:** در این روش،نفوذگر به همه داده‌های تبـادلی روی شبکه گوش می‌کند تا پیام مناسبی را که از سمت یک ایستگاه به سمت سرور رفته است،پیدا کند.

۳- **تحلیل ترافیک :** روشی دیگری برای حمله که در آن هکر، ترافیک شبکه را تحلیل می‌کند تا الگوی کلی شبکه را به دست بیـاورد. وی با این کار متوجه می‌شود که دقیقاً هر ایستگاه کاری چه کار می‌کند و چگونه کار می‌کند.

◄ WEP(Wired Equivalent Privacy)

در اين روش، از شنود كاربرهايي كه در شبكه مجوز ندارند جلوگيري به عمل مي آيدكه منـاسب براي شبكه هاي كوچك است، زيرا نيـاز به تنظيمـات دستي(KEY) مربوطه در هرClient مي باشد.

◄ SSID (Service Set Identifier)

شبكه هاي WLAN داراي چنـدين شبكه محلي مي بـاشند كه هركدام آنهـا داراي يك شنـاسه (Identifier) يكتـا مي بـاشند.
اين شنـاسه ها در چنـدين Access Point قرار داده مي شوند.هر كـاربر براي دسترسي به شبكه موردنظربايستي تنظيمات شناسه SSID مربوطه را انجام دهد.

◄ MAC (Media Access Control)

ليستي از MAC آدرس هاي مورد استفاده در يك شبكه به (AP (Access Point مربوطه وارد ميشود.بنـابراين تنها كـامپيوترهاي داراي اين MAC آدرسهـا اجازه دسترسي دارند،به عبـارتي وقتي يك كـامپيوتر درخواستي را ارسـال مي كند MAC آدرس آن با ليست MAC آدرس مربـوطه در AP مقايسه شده و اجـازه دسترسي يا عدم دسترسي آن مورد بررسي قرار مي گيرد.

<u>پنج گام براي داشتن يك شبكه بي‌سيم ايمن</u>

◄ 1- استفاده از شبكه‌هاي آشنا

- **2- فهرست‌بندي دقيق اولويت‌ها**
- **3- فعال‌سازي گزينه امنيت روي روتر**
- **4- انتخاب يك رمز عبور مناسب**
- **5- فعال كردن امنيت Web - mail**

سناریوی کلی در هر ارتباط امن

- نیاز انتقال یک پیام بین طرفین با استفاده از یک کانال نا امن (مثل شبکه اینترنت)
- نیاز به تامین سرویسهای محرمانگی، تمامیت و احراز هویت در انتقال پیام
- تکنیکهای معمول مورد استفاده :
  - تبدیل امنیتی :
    - جهت فراهم آوردن سرویسهای امنیتی مورد نیاز
  - اطلاعات مخفی:
    - در تبدیل فوق استفاده می شوند
    - به نحوی بین طرفین ارتباط به اشتراک گذاشته می شوند.

جهت فراهم آوردن سرویس امنیتی خاص مدل ارائه شده:

- طراحی الگوریتم مناسب برای انجام تبدیل امنیتی مورد نظر
- تولید کلیدهای مخفی مورد نیاز طرفین
- استفاده از روش مناسب برای توزیع و توافق درباره اطلاعات مخفی
- طراحی یک پروتکل مناسب برای ارتباط طرفین و تضمین سرویس امنیتی

- **شما هم می توانید کلمه عبور شبکه های بیسیم Wi-Fi را هک کنید پس مراقب باشید**

- **هرگز از سیستم رمزگذاری WEP برای شبکه بیسیم خود استفاده نکنید! می پرسید چرا؟ یکی از مشکلات عمده شبکه های بیسیم در ایران، عدم توجه لازم به امنیت آنها است و البته وضعیت مودم های ADSL بیسیم که این روزها به شکل**

گسترده ای مورد استفاده قرار می گیرند، از آن هم بدتر است. تا به حال امتحان کرده اید که در محل کار و یا زندگی تان چند شبکه بیسیم سرگردان بدون هیچ گونه کلمه عبور و محافظی وجود دارد؟

در این مطلب قصد داریم بصورت مرحله به مرحله روش دستیابی به کلمه عبور یک شبکه بیسیم را با هم امتحان کنیم. اما قبل از آن نکته مهمی را باید بازگو کنم: دانش، قدرت است. اما قدرت به این معنی نیست که ما باید به آدم بدی تبدیل شویم و به هر کار غیر قانونی دست بزنیم. دانستن نحوه باز کردن قفل که شما را تبدیل به یک دزد نمی کند. پس لطفا این مطلب را یک مقاله آموزشی و یک تمرین خلاقیت فکر بدانید.

WiFi Direct

- این استاندارد به کلاینت‌ها کمک می‌کند بدون نیاز به یک اکسس‌پوینت واقعی به یکدیگر متصل شوند. به زبان ساده، یک تلفن‌هوشمند، خود را به یک اکسس‌پوینت کوچک تبدیل می‌کند تا سایر دستگاه‌ها به آن متصل شوند. این استاندارد برای به اشتراک‌گذاری اینترنت با چند دستگاه دیگر فوق‌العاده مفید است.
- این استاندارد به کلاینت‌ها کمک می‌کند بدون نیاز به یک اکسس‌پوینت واقعی به یکدیگر متصل شوند. به زبان ساده، یک تلفن‌هوشمند، خود را به یک اکسس‌پوینت کوچک تبدیل می‌کند تا سایر دستگاه‌ها به آن متصل شوند. این استاندارد برای به اشتراک‌گذاری اینترنت با چند دستگاه دیگر فوق‌العاده مفید است.

بهینه‌سازی شبکه وای‌فای به کمک موقعیت و تجهیزات

- پوشش سیگنال
- بهترین عملکرد سیگنال‌های وایرلس در محیط‌های باز است. به خاطر اینکه فراهم کردن محیط‌هایی تا این حد باز در ساختمان غیرممکن است، می‌توانید وضعیت روتر را به گونه‌ای تنظیم کنید که از کیفیت و قدرت سیگنال‌های آن در جهت‌هایی خاص اطمینان حاصل کنید. این نکته به این معناست که شما نباید روتر را مثلاً در کمد لباس‌ها (!!) یا بین تلویزیون و دیوار قرار دهید. بهترین مکان برای قرارگیری دستگاه، جایی در میانه‌های فاصله سقف تا کف است. اما انجام اینکار سخت است. در نتیجه بهترین جایگزین، قرار دادن آن بر روی وسایلی مانند میز یا نصب‌کردن آن بر روی دیوار است. به طور کلی هر شئ فیزیکی از قبیل دیوار، ظرفهای بلورین یا غیره با شدت و ضعف‌های متفاوت سیگنال‌ها را ضعیف می کنند.

بهینه‌سازی شبکه وای‌فای به کمک موقعیت و تجهیزات

- **موقعیت قرارگیری آنتن**
- به کمک روترهایی که دارای آنتن خارجی هستند به راحتی می توانید حجم کُره ایجاد شده (یعنی همان پوشش سیگنال‌ها) را افزایش داد. به طور معمول کاربران آنتن را به صورت عمودی نصب می‌کنند؛ چرا که هدف آنها پخش‌شدن سیگنال‌ها در محیط است. اگر قصد دارید سیگنال‌های شبکه را در عمق ارسال کنید، آنتن را به صورت افقی نصب کنید. توجه داشته باشید که این ترفند در تمامی روترها کاربردی نیست. در بعضی روترها جابه‌جایی یا تنظیم آنتن در راستاهای مختلف تغییر زیادی ایجاد نمی کند.
- اگر آنتن قابل جدا شدن باشد، می توان آنرا با یک آنتن گیرنده قدرتمندتر تعویض نمود (در واقع آنتن قوی‌تر، یک آنتن بزرگتر است). همین امر باعث افزایش قابل توجه پوشش سیگنال می‌شود. علاوه بر این می توانید با پیچاندن ورقه‌های نازک (فویل) آلومینیوم به قسمت قوس‌دار آنتن، قدرت آن را به طور چشمگیری افزایش دهید. برای افزایش قدرت و پوشش روترهای دارای آنتن داخلی کاری نمی‌توان کرد.

- **روتـر**

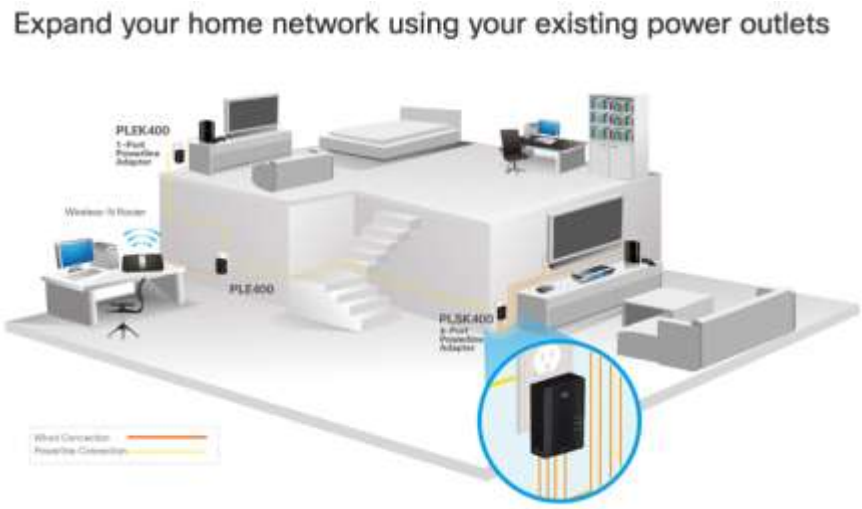
در حال ایده‌آل شما فقط به یک دستگاه بردکست‌کننده در منزل نیاز دارید. برای اغلب منازل یک روتر کافی و مناسب است. اگر منزل کوچکی دارید و با وجود قرارگیری روتر در بهترین مکان ممکن (یعنی مرکز) باز هم پوشش کافی در سراسر خانه ندارید شاید بهتر باشد، دستگاه خود را تعویض کنید. پیشنهاد ما انتخاب حداقل یک روتر N600 است. اما اگر این میزان هزینه کردن را به صرفه نمی‌دانید، گزینه‌های دیگری نیز در بازار یافت می‌شود.

- **اکسس‌پوینت**

اکسس‌پوینت جداگانه، یک راهکار ایده‌آل برای خانه‌های بزرگ محسوب می‌شود. یعنی در مواردی که قرارگیری یک روتر در مرکز ساختمان، جوابگوی نیازهای کاربر نیست. اصولا زمانی از اکسس‌پوینت اضافی استفاده می شود که سیگنال‌های روتر به بخشهای خاصی نرسیده یا ضعیف

باشند. یک مثال کاربردی در این زمینه قرارگیری روتر در سالن و اکسس‌پوینت در طبقه زیرین است.

- اگر این راهکار بهترین حالت ممکن تشخیص داده شد، حالا زمان اتصال اکسس‌پوینت به روتر است. اساساً برای اتصال روتر به اکسس‌پوینت از کابل شبکه استفاده می‌شود. اما اگر این اتصال نیازمند صرف زمان و هزینه غیرمنطقی است، می‌توان از شبکه‌های موسوم به Power Lineبهره گرفت.



شبکه‌هایPower Line

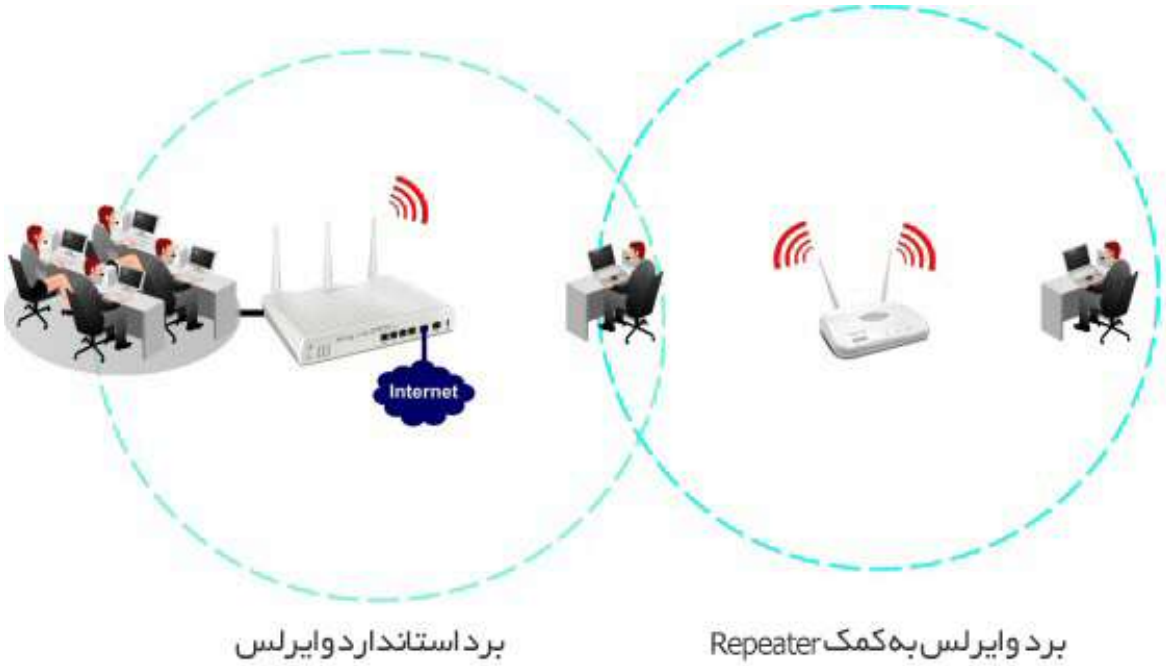
- وقتی صحبت از شبکه می‌شود، نمی‌توان همیشه به کابل شبکه دسترسی داشت. از طرف دیگر دریافت سیگنال‌ها در بعضی از قسمت‌های ساختمان به علت فاصله زیاد از اکسس‌پوینت، ممکن است ضعیف باشد. در این موارد بهترین راهکار استفاده از یک جفت آداپتور Power Line است.

- آداپتورهایPower Line ، سیم‌کشی‌های الکتریکی ساختمان را به کابل شبکه تبدیل می‌کنند. برای استفاده از این ویژگی به دو آداپتور نیاز دارید. یکی از این دو به اکسس‌پوینت (یا روتر) و دیگری به کلاینت Ethernet-Ready متصل خواهد شد.

- در حال حاضر دو استاندارد HomePlug AV و Powerline AV+ 500 برای Power Line وجود دارد که به ترتیب سرعت اتصال ۲۰۰ و ۵۰۰ مگابایت در ثانیه را فراهم می‌کنند.

افزایش دهنده برد / (Range Extender) تکرارکننده(Repeater)

- **این دو دستگاه بی‌سیم، می‌توانند به یک شبکه وای‌فای فعال متصل شده و سپس سیگنال‌های آن را به فاصله دورتری ارسال کنند. به عبارت دیگر، برای افزایش برد یک شبکه، از این دو دستگاه استفاده می‌شود. اغلب مدل‌های این دستگاه‌ها، از تنظیمات شبکه های وای‌فای پشتیبانی کرده و تنها با فشردن یک کلید می‌توانند به روتر فعال در شبکه متصل شوند. بعد از اتصال تنها کافی است Repeater را در انتهای برد سیگنال‌های شبکه (مرز کُره فرضی) قرار دهید تا برد شبکه افزایش یابد.**



با اینکه استفاده از این دستگاه‌ها بسیار متداول است، اما به دلایل زیر استفاده از آن‌ها توصیه نمی‌شود:

- **الف) معیار دقیقی برای سنجش مؤثر بودن آن‌ها در افزایش برد سیگنال‌های شبکه وجود ندارد. کاربر باید محلی را برای قرارگیری Repeater انتخاب کند که از طرفی برای اتصال دستگاه به روتر به اندازه کافی به آن نزدیک باشد و از طرف دیگر آنقدر دور باشد که بتواند برد سیگنال را افزایش دهد. پیدا کردن موقعیتی که هم منجر به اتصال پایدار دستگاه به روتر و هم منجر به افزایش برد سیگنال‌ها بشود کار بسیار سختی است.**

- **ب) اساساًRepeater ، شبکه وای‌فای موجود را کپی می کند. از طرفی همانگونه که پیشتر اشاره شد، سیگنال‌های وای‌فای در همه جهت ها ارسال یا بردکست (Broadcast) می‌شوند. با توجه به این دو ویژگی دستگاه‌هایی که در محدوده هم‌پوشانی سیگنال‌های هر دو شبکه (شبکه اصلی و شبکه ایجاد شده توسط (Repeater قرار دارند، مجبورند با سیگنال‌های مزاحم شبکه دیگر کنار بیایند. تأثیر بد این مسأله در شبکه‌هایی با فرکانس ۲,۴ گیگاهرتز دو چندان است.**

- **یکی از مشکلات رایج در شبکه‌های وای‌فای، خطر سوءاستفاده کاربران غیرمجاز از پهنای باند شبکه است. در این بخش به شیوه ایمن‌سازی شبکه و بهینه‌سازی آن برای افزایش سرعت خواهیم پرداخت. توجه داشته باشید که این توضیحات برای کسانی مناسب است که علاقمند به یادگیری بیشتر در مورد شبکه هستند. از این رو ممکن است بخش‌هایی از مطالب برای کاربران مبتدی، تا حدودی تخصصی و سطح بالاتر باشد.**

- ***توضیح: توصیه اکید میکنیم که قبل از انجام کار، از تنظیمات و پیکربندی روتر خود پشتیبان تهیه کنید. این کار به شما امکان می‌دهد که در صورت وقوع خطا یا بروز اخلال در پیاده‌سازی پیکربندی جدید به راحتی بتوان تنظیمات به حالت قبل بازگرداند .***

- **به استثناء تجهیزات شبکه تولید شده توسط کمپانی اپل، تقریباً تمامی روترها و اکسس‌پوینت‌های موجود در بازار به یک رابطکاربری مبتنی بر وب مجهز هستند. این ویژگی بدان معنا است که به کمک مرورگر یک رایانه متصل به دستگاه و تایپ کردن آی‌پی آدرس، میتوان صفحه مدیریت روتر را اجرا کرد. در حالت پیش‌فرض، IP Addressروتر، در پایین روتر یا در بخش راهنمای کاربر (User Guide) چاپ شده است.**

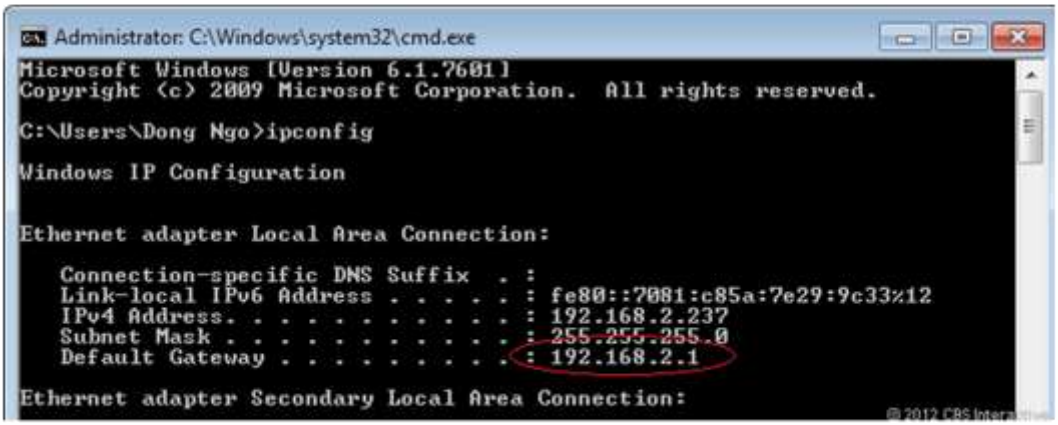
- **برای ورود به رابطکاربری تنظیمات روتر، می‌توان مراحل زیر دنبال نمود:**

- **گام نخست: در یک رایانه متصل به دستگاه و به کمک دستورCMD ، سرویس Command Promptرا اجرا کنید.**

- ***توضیح: برای اجرای Command Promptدر سیستم‌عامل ویندوز اکس‌پی، بر روی منوی استارت کلیک نموده و بعد از اجرای سرویسRun ، دستور CMDرا تایپ و کلید اینتر را بفشارید. در نسخه‌های بالاتر از اکس‌پی، دستور CMDرا در منوی استارت تایپ کرده و کلید اینتر را بفشارید .***

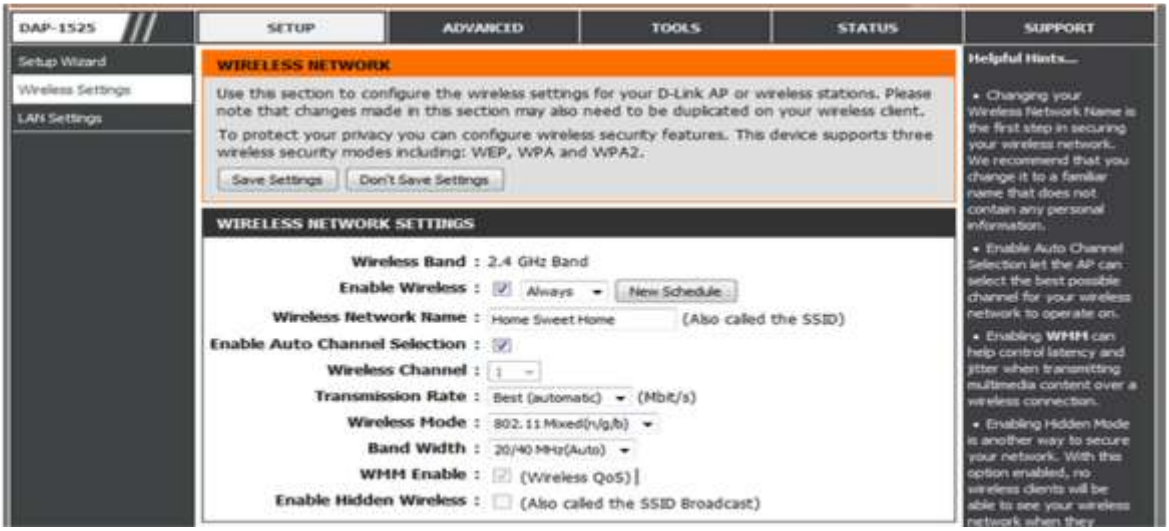
بهینه سازی شبکه وای‌فای به کمک تنظیمات وای‌فای

- گام دوم: در پنجره باز شده، دستور ipconfig را تایپ و کلید اینتر را فشار دهید. با انجام این کار اطلاعات زیادی بر روی صفحه نمایش داده می‌شود. شما باید به دنبال رشته‌ای از اعداد بگردید که در مقابل عبارت Default Gateway درج شده است. این رشته از اعداد در حقیقت آی‌پی آدرس روتر شما محسوب می‌شود.



بهینه سازی شبکه وای‌فای به کمک تنظیمات وای‌فای

- گام سوم: آی‌پی آدرس یاد شده را در آدرس بار مرورگرتان وارد نموده و کلیک اینتر را بفشارید. حالا شما در رابطکاربری مبتنی بر وب روتر هستید. در ادامه باید با یک حساب کاربری وارد بخش تنظیمات شوید. نام کاربری, در اغلب موارد admin است. برای کلمه‌عبور نیز به دفترچه راهنمای روتر مراجعه نموده و یا آن را از فردی که برای اولین بار روتر را راه‌اندازی نموده است سؤال کنید.



در رابطکاربری، دنبال نمودن تنظیمات وایرلس(Wireless Settings) ، به شما در ایمن نگاه‌داشتن شبکه کمک می‌کند. تعدادی از بخشهای تنظیمات وایرلس به شرح زیر هستند:

- **نام شبکه (Network Name) و کلمه‌عبور (Password)**

تقریباً تمامی روترها با یک نام شبکه (یا (SSID و کلمه‌عبور پیش‌فرض عرضه می‌شوند. بهتر است نام شبکه و کلمه‌عبور پیش‌فرض را تغییر دهید. چراکه از یک طرف نام شبکه و کلمه‌عبور پیش‌فرض برای هکرهای حرفه‌ای و آشنا به این گونه تجهیزات، کاملاً قابل حدس بوده و از طرف دیگر می‌توانید نام‌هایی انتخاب کنید که به خاطرسپاری آنها برای شما راحت‌تر باشد.

- **مخفی کردن SSID**

در حالت پیش‌فرض تمامی روترها، نام شبکه وای‌فای را بردکست میکنند. با این کار کلاینت‌ها به راحتی می‌توانند شبکه‌های پیرامون خود را ببینند. مخفی کردنSSID ، شبکه وای‌فای شما را نامرئی (Invisible) میکند. تنها ضعف مخفی کردن SSID این است که در هنگام جستجو برای اتصال به شبکه، نام شبکه نمایش داده نشده و خودتان باید آن را تایپ کنید. البته به جای این کار می‌توانید برای مدتی کوتاه SSID را روشن کنید و بعد از اتصال کلاینت جدید، مجدداً آن را مخفی کنید.

- **استفاده از WPA 2**

استفاده از متد رمزنگاریWPA 2 ، علاوه بر بالا بردن امنیت شبکه، باعث افزایش سرعت سیگنال‌های وای‌فای نیز می‌شود. البته WPA 2 ممکن است با کلاینت‌های قدیمی‌تر سازگار نباشد. اکثر کلاینت‌هایی که در چند سال اخیر به بازار آمده‌اند از این متد پشتیبانی می‌کنند. بهتر است در ابتدای امر از WPA 2 استفاده کنید. اگر در ادامه کلاینت‌هایی قادر به استفاده از شبکه نبودند، مجدداً متد رمزنگاری را به WPA بازگردانید (در نظر داشته باشید که WPA از امنیت بسیار پایینی برخوردار است و براحتی با استفاده از نرم‌افزارهای ساده هک، می‌توان به آنها نفوذ کرد.(

- **درکنار موارد فوق، گزینه‌های دیگری در بخش تنظیمات وایرلس وجود دارد که شما قادر به مشاهده و ایجاد تغییر در آنها هستید. البته برای حفظ سلامت دستگاه و جلوگیری از بروز مشکلات اتصال، بخش‌هایی مانند MAC Address و اینترنت نمایش داده نمی‌شوند. دسترسی به این بخش‌ها معمولاً در حالت پیشرفته (Advanced) امکان‌پذیر است.**

- **وای‌فای و اینترنت، دو چیز کاملاً متفاوت هستند .**

با افزایش محبوبیت شبکه‌های بی‌سیم، لفظ وای‌فای اغلب با اینترنت مترادف شده و بعضی کاربران از عبارت وای‌فای به معنای اتصال(Connection) های اینترنت یاد می‌کنند. در ادامه این مقاله، سعی داریم، این دیدگاه را اصلاح نموده و با تعاریف مرتبط، بهتر و دقیق‌تر آشنا شویم. این مسأله به ما در شناسایی بهتر خطاها و افزایش سطح آگاهی کمک بسیاری شایانی می‌کند.

مقایسه انواع بسترهای اینترنت

فناوری	WiMAX	WiFi	xDSL
برد قابل دسترسی	-طراحی شده برای ارسال اطلاعات در حدود ۶ تا ۱۰ کیلومتر بدون نیاز به دید مستقیم -قابلیت افزایش برد تا ۵۰ کیلومتر با دید مستقیم	-طراحی شده برای پشتیبانی از مسافتی در حدود ۱۰۰ متر -اضافه کردن Access Point و استفاده از آنتن پیشرفته تر برد قابل دسترسی را افزایش می دهد. -بدون دید مستقیم	-طراحی شده برای پشتیبانی از مسافتی در حدود ۱ تا ۵ کیلومتر
مدولاسیون	- ۲۵۶ sub-carrier OFDM using ۶۴-QAM ،QPSK ،۱۶-QAM	- QPSK	- DMT
سرعت انتقال	-بیش از ۷۵Mbps در یک کانال ۲۰MHz ،۳.۸ bps/Hz	-بیش از ۵۴Mbps در یک کانال ۲۰MHz ،۲.۷ bps/Hz	- تا ۸Mbps غیر متقارنADSL - تا ۳Mbps متقارن SHDSL - تا ۵۲Mbps متقارنVDSL
کیفیت خدمات(QOS)	- Grant-request MAC -تضمین پهنای باند برای کلیه سرویس های قابل انتقال مانندData ،Video وVoice بروی شبکه Access ،DSL وWiMAX -ارائه سرویس در تمامی سطوح امکان پذیر است. -کاملا ایده آل برای شرکت ها و سازمان های بزرگ -متقارن یا HFDD/FDD/TDD نامتقارن	- CA/CSMA Contention ،۸۰۲.۱۱e –based MAC -در تلاش برای به دست آوردن آن قابلیت می باشد. - TDD -فقط با متقارن -امکان ارائه سرویس در تمامی سطوح وجود ندارد.	QOS -پشتیبانی شده برای صدا و تصویر و اطلاعات -فقط مناسب برای کاربران خانگی

i

منابع

ماهنامه شبکه شماره 50 و 56

http://irancell.ir/portal/home

http://wimaxnews.ir

http://www.zoomit.ir

http://en.wikipedia.org/wiki/WiMAX

wimax.blogfa.com (Iran WiMAX)

http://www.farazrco.ir/post/25

www.gorgancsg.ir