بسم الله الرحمن الرحیم

- ضروری‌ترین اقدامات ایمنی روی مودم‌های وایرلس
- اطلاعات پایه امنیت در شبکه
- تست حافظه‌ی رم در رایانه

منبع: ماهنامه‌ی فرهنگ سربازی شماره‌های ۲۰(۹۰)(۸۰)

مدیریت تنظیمات

اولین قدم برای افزایش امنیت شبکه، دسترسی به بخش مدیریتی مودم یا روتر برای پیکربندی آن است. اغلب هنگامی که رایانه خود را با استفاده از کابل به مودم یا روتر متصل می‌کنید، سرور DHCP روی مودم یک آی‌پی به دستگاه شما اختصاص داده و شما می‌توانید با وارد کردن آدرس Gateway در مرورگر خود به صفحه مدیریت مودم وارد شوید. آدرس پیش‌فرض گیت‌وی نیز در راهنمای سریعی که همراه مودم ارائه می‌شود قابل مشاهده بوده و در بیشتر موارد ۱۹۲,۱۶۸,۱,۱ یا ۱۹۲,۱۶۸,۰,۱ است. همچنین به نام کاربری و رمز عبور پیش‌فرض برای ورود به این بخش نیز در همان راهنما اشاره شده و در اغلب موارد عباراتی همچون admin, admin یا admin, password یا نام کاربری admin و فاقد رمز عبور است.

قدم اول: تغییر رمز مدیریت

اولین اقدام پس از ورود به بخش پیکربندی مودم، تغییر نام کاربری و رمز عبور پیش‌فرض دستگاه است. برای انجام این کار معمولا باید ابتدا به بخش تنظیمات حرفه‌ای (Advanced) مراجعه کرده سپس دنبال گزینه‌هایی مشابه با System, Management, User یا Maintenance باشید. پس از پیدا کردن گزینه موردنظر، کاربران مجاز برای دسترسی به بخش تنظیمات به‌نمایش درآمده و می‌توانید نسبت به تغییر نام کاربری یا رمزعبور اقدام کنید.

قدم دوم: تغییر نام شبکه بی‌سیم

متاسفانه برخی کاربران به نام شبکه بی‌سیم خود توجهی ندارند و این نام نیز در اغلب موارد نام یا مدل مودم یا روتر است و براحتی می‌توان با شناسایی حفره‌های امنیتی موجود در فریمور دستگاه به آن

نفوذ کرد. بـــرای تغییر نام شـــبکه وای‌فای که همان SSID اســـت پس از ورود بـــه بخش مدیریت گزینه Wireless یا Wireless Lan را جســـتجو کرده و در تنظیمـــات مربوط به آن مقـــدار موجود در بخش SSID را به عبارت دلخواه خود تغییر دهید. (از انتخاب نام یا نام خانوادگی خود پرهیز کنید)

قدم سوم: فعال‌سازی رمز اتصال

شاید از میان ده‌ها و حتی صدها شبکه وای‌فای تمام آنها به رمز اتصال مجهز باشند، اما مطمئنا از میان هزار شبکه در سطح شهر براحتی می‌توانید یک شبکه فاقد رمزعبور نیز پیدا کنید! اختصاص رمزعبور و فعال‌سازی الگوریتم‌هـــای رمزنگاری اطلاعـــات از دیگر اقدامات مهم برای افزایش امنیت شـــبکه وای‌فای است. برای انجـــام این کار به صفحه تنظیمـــات وایرلس در مودم مراجعه کرده و در بخش Security Mode یکی از گزینه‌های شامل WPA یا WPA2 را انتخاب کنید.

در ادامه در کادر مرتبط با رمز عبور یک رمزعبور پیچیده شـــامل عدد و حـــرف را وارد و به‌این‌ترتیب رمز اتصال به شـــبکه را مشخص کنید. (از اختصاص شماره تلفن، شـــماره موبایل، کدپســـتی، نام و نام خانوادگی یا حتی تکرار دو یا ســـه مرتبه سال تولد خودداری کنید، چراکه این رمزها گزینه‌های قابل حدس زدن به‌شمار می‌روند)

قدم چهارم: غیرفعال‌سازی WPS

برخـــی از روترها و مودم‌هـــای وایرلس از قابلیتی با عنوان WPS پشتیبانی می‌کنند. به‌کمک این قابلیت که به‌صورت یک دکمه روی مودم تعبیه شـــده اســـت کاربران می‌توانند بدون نیاز به رمزعبور و با فشار دکمه روی مودم و ارســـال درخواســـت اتصال روی دستگاه هوشـــمند یا رایانه خود، اتصال امن و خودکار را تجربه کنند. این قابلیت گرچه مفید اســـت، اما موارد زیادی از

وجود حفره‌های امنیتی در آن گزارش شده و پیشنهاد می‌شود برای افزایش امنیت شبکه خود ضمن مراجعه به تنظیمات مودم یا روتر، گزینه WPS را جستجو کرده و آن را غیرفعال کنید. (این گزینه ممکن است در صفحه تنظیمات وایرلس باشد)

قدم پنجم: فیلترگذاری روی مک

همان‌طور که پیشتر نیز اشاره کردیم، آدرس مک یک آدرس فیزیکی منحصر به‌فرد مربوط به کارت شبکه است و هیچ‌گاه نمی‌توانید دو آدرس مک مشابه در تجهیزات تولیدی توسط شرکت‌های مختلف پیدا کنید. این منحصربه‌فرد بودن آدرس مک و دشوار بودن مراحل شبیه‌سازی یک آدرس جعلی موجب

شده است آدرس‌های مک به‌عنوان یکی از بهترین گزینه‌های امنیتی در شبکه‌های بی‌سیم کاربرد داشته باشند. تقریبا می‌توان گفت تمام تجهیزات شبکه‌های بی‌سیم از قابلیت فیلترگذاری روی آدرس مک پشتیبانی می‌کنند که به کمک این قابلیت می‌توانید فهرست سفید یا فهرست سیاهی از آدرس‌های مک را ایجاد کنید. آدرس‌های وارد شده در فهرست سیاه دستگاه‌هایی را شامل می‌شود که اجازه اتصال به مودم یا روتر را ندارند و آدرس‌های وارد شده در فهرست سفید نیز به‌این معناست که فقط دستگاه‌های موجود در این فهرست قادر به اتصال به شبکه است.

استفاده از این روش شاید در نگاه اول کمی پیچیده یا وقتگیر باشد (مرحله پیدا کردن آدرس مک

دستگاه‌های مختلف ممکن است کمی زمانبر باشد)، اما باتوجه به میزان امنیتی که در اختیار شما قرار می‌دهد مهم‌ترین، ضروری‌ترین و بهترین روش برای افزایش امنیت شبکه‌های بی‌سیم به‌شمار می‌رود. همچنین این نکته را فراموش نکنید که پس از فعال‌سازی فهرست سفید برای آدرس‌های مک، در صورتی که دیگر کاربران رمز اتصال به شبکه شما را نیز در اختیار داشته باشند قادر به اتصال به آن نخواهند بود!

برای فعال‌سازی این قابلیت باید در صفحه تنظیمات وایرلس یا در بخش Security گزینه‌ای با عنوان Mac Filter را جستجو کنید. با مراجعه به این بخش و فعال‌سازی قابلیت Mac Filter می‌توانید هریک از گزینه‌های فهرست سفید (Allow) یا فهرست سیاه (Deny) را فعال کرده و در جدول

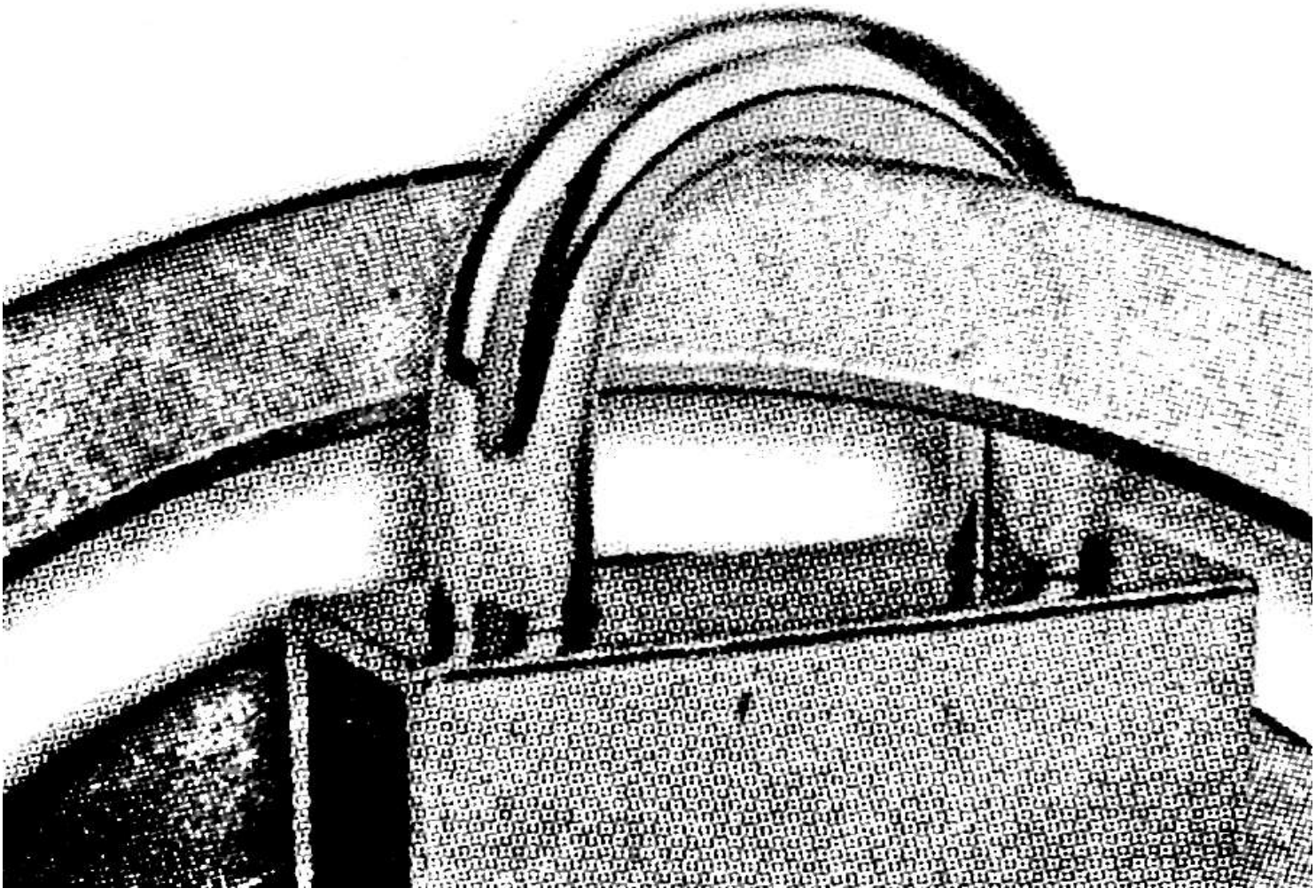
به‌نمایش درآمده آدرس‌های مک دستگاه‌هایی را که قصد دارید به شبکه متصل شوند یا مانع اتصال آنها شوید مطابق فرمت مشخص شده وارد کنید.

برای مثال چنانچه قصد دارید فهرست سفید را فعال کنید و یک رایانه رومیزی، یک لپ‌تاپ و دو تلفن همراه توسط ارتباط بی‌سیم به شبکه وای‌فای شما متصل می‌شوند، باید پس از انتخاب گزینه Allow، آدرس مک مربوط به چهار دستگاه مورد اشاره را در خانه‌های جدول به‌نمایش درآمده وارد کنید.

مک کجاست؟

پرسشی که بسیاری از کاربران در ذهن خود دارند این است که آدرس مک کجاست و چطور می‌توان به آن دسترسی داشت؟ آدرس مک در بسیاری از موارد روی بسته‌بندی تجهیزات شبکه به‌صورت بارکد به‌چاپ رسیده و گاهی نیز با بازکردن در باتری (قاب پشت)

دستگاه‌های هوشمند همچون تلفن همراه و تبلت می‌توان آن را مشاهده کرد. همچنین آدرس مک کارت شبکه وایرلس در لپ‌تاپ‌ها را نیز می‌توان روی بارکدهای چسبیده شده به زیرلپ‌تاپ یا روی کارتن آن مشاهده کرد، اما علاوه بر این روش‌ها، به کمک روش‌های نرم‌افزاری نیز می‌توان آدرس مک را به‌دست آورد.



ویندوز

۱ـ به منوی استارت مراجعه کرده و در کادر جستجو عبارت ncpa.cpl را وارد کرده و کلید اینتر را فشار دهید.

۲ـ در پنجره به‌نمایش درآمده همه اتصالات موجود بجز اتصال مربوط به وایرلس (Wireless Network Connection) را غیرفعال کنید. (برای انجام این کار باید روی اتصال موردنظر کلیک راست ماوس را فشار داده و گزینه Disable را انتخاب کنید)

۳ـ به منوی استارت بروید و در کادر جستجو عبارت CMD را وارد کرده و کلید اینتر را فشار دهید.

۴ـ در خط فرمان عبارت getmac را وارد کرده و کلید اینتر را بزنید.

۵ ـ در فهرست نتایج ممکن است گزینه‌های مختلفی برای شما نمایش داده شود که در مقابل آنها عبارت Disabled یا Disconnected وجود دارد. بجز این گزینه‌ها یک گزینه شامل آدرس فیزیکی خواهد بود که این آدرس همان آدرس مک متصل به کارت شبکه بی‌سیم شماست.

مگ...

ystem Preferences ۱ـ از منوی اصلی به

مراجعه کرده و به بخش Network وارد شوید.

۲ـ گزینه Wi-Fi را از فهرست به‌نمایش درآمد

در ستون سمت چپ انتخاب کرده و از سمت راست

از فرمان‌هـــای زیـــر را در آن وارد کنیـــد
(باتوجه به سیستم‌عامل مورد اســـتفاده فرمان‌ها
متفاوت است):

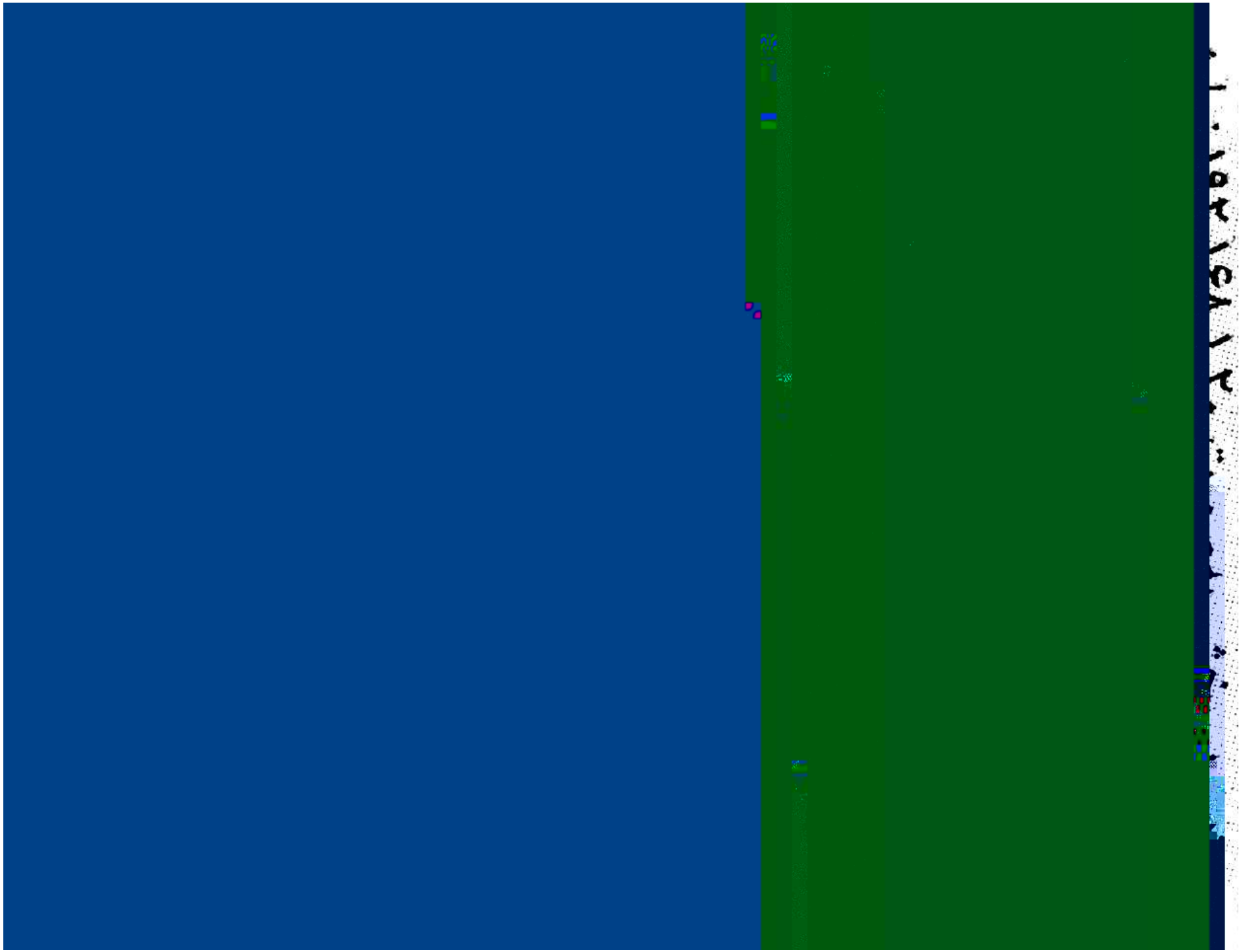
fconfig/

sbin/i

netstat –in

۳ـ به بخش About Phone رفته و در همین
Status

برای افزایش امنیت در شبکه بهتر است با برخی اصطلاحات و واژه‌ها در شبکه‌های کابلی یا بی‌سیم آشنا باشید



بوده و گزینه تکراری در آنها وجود ندارد. (با استفاده از روش‌های نرم‌افزاری می‌توان این آدرس‌ها را نیز به‌صورت مجازی شبیه‌سازی کرد)

آدرس‌های مک توسط شش جفت کاراکتر هگزادسیمال نشان داده می‌شوند که میان هر جفت کاراکتر نیز ممکن است علامت دو نقطه، خط تیره یا نقطه وجود داشته باشد. به‌عنوان مثال آدرس 98:6c:f5:3d:77:ef یک آدرس منحصربه‌فرد فیزیکی یا همان آدرس مک است. باتوجه به منحصربه‌فرد بودن این آدرس‌ها، بهترین گزینه برای پالایش اتصالات

Gateway

هنگامی که چند دستگاه به یک روتر یا سوئیچ

در شبکه برخوردار خواهند بود. (تفاوتی در اتصالات

کابلی و وایرلس در یک شبکه محلی وجود ندارد)

DHCP

سرور دی‌اچ‌سی‌پی در روترها یا دیگر تجهیزات شبکه مسئولیت اختصاص آدرس آی‌پی به دستگاه‌های موجود در شبکه را عهده دار است. به‌این ترتیب هر دستگاه یک آدرس آی‌پی

منحصربه‌فرد را در شبکه محلی دریافت می

احتمال تداخل آی‌پی به‌دلیل وجود دو آدرس یا

به صفر می‌رسد.

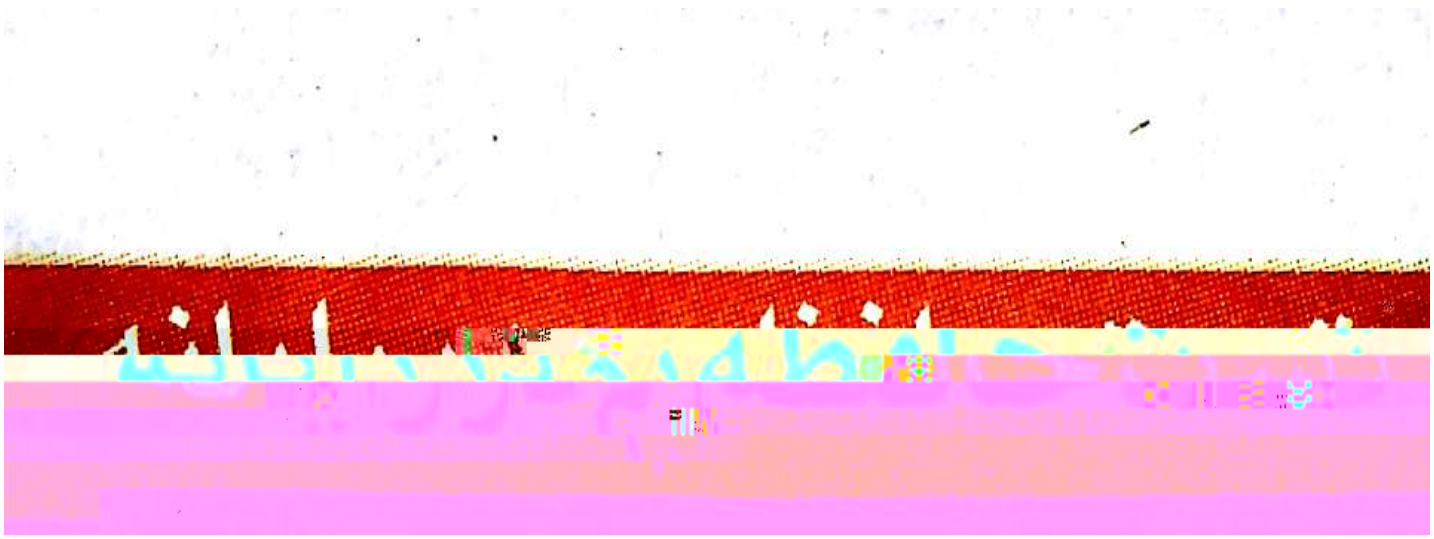
SSID

همان‌طور که می‌دانید شبکه‌های وای‌فای

اسمی که به آنها اختصاص داده شده است ش

شده و عملیات اتصال به آنها صورت می گیرد

نام SSID گفته می‌شود.



مشکلات مربوط به حافظه رم (Ram) در سیستم‌های رایانه‌ای از مشکلاتی به‌شمار می‌رود که بررسی و تشخیص آنها کار نسبتا دشواری است؛ اما این بررسی نسبتا دشوار به کمک ابزارهای موجود در ویندوز و ابزارهایی که به همین منظور طراحی شده‌اند، براحتی امکان‌پذیر است و هر کاربری با کمی آشنایی با این ابزارها می‌تواندخیلی آسان مشکلات موجود در رم را شناسایی کند.

در ادامه قصد داریم شما را با دو روش (ابزار موجود در ویندوز و نرم‌افزار قدرتمند MemTest86) آشنا کنیم.

تست ویندوزی

* منوی استارت را باز کرده و در کادر جستجو عبارت Windows Memory Diagnostic را وارد کنید. سپس گزینه به‌نمایش درآمده با همین عنوان را کلیک کنید تا

ابزار موردنظر اجرا شود.

* همه برنامه‌های فعال در ویندوز را ببندید و گزینه Restartnowandcheckforproblems (recommended) را در پنجره به‌نمایش درآمده انتخاب کنید.

* اکنون رایانه شما به‌طور خودکار ری‌استارت شده و ابزار تست حافظه پیش از بوت ویندوز فعال می‌شود و به‌طور خودکار حافظه رم را

عملیات تست، رایانه دوباره ری‌استارت و ویندوز بوت شود.

* پس از بوت مجدد ویندوز، گزارشی از تست انجام شده در اختیار شما قرار می‌گیرد که با بررسی آن می‌توانید به مشکلات احتمالی پی ببرید.

نکته: در صورتی که گزارش موردنظر پس از ری‌استارت قابل مشاهده نبود می‌توانید با فشار کلیدهای Win+R و تایپ عبارت eventvwr.msc ابزار گزارش‌گیری ویندوز را اجرا کنید. سپس از سمت چپ گزینه Windows Logs و در ادامه System را انتخاب کرده و روی گزینه Find در سمت راست کلیک کنید. عبارت MemoryDiagnostic را در کادر جستجو وارد کنید و در فهرست نتایج آخرین گزارش‌های موجود را برای بررسی نتیجه تست حافظه رم مشاهده کنید.

MemTest86

استفاده از این ابزار نیز بسادگی استفاده از ابزار موجود در ویندوز است. به لینک زیر مراجعه کرده و در بخش MemTest86 V7.0 Free Edition، یکی از فایل‌های قابل رایت روی دیسک نوری یا قابل

ذخیره‌سازی روی فلش را دانلود کنید:

http://www.memtest86.com/download.htm

در ادامـــه در صورتی که فایل ISO را دانلود کردید

با استفاده از ابزارهای رایت دیسک نوری آن را روی

آغای! فابیوس

صدای من را می‌شنوید؟!

من از ایران حرف می‌زنم، کشوری که به آن خون‌های آلوده به ایدز صادر کردید.

اینجا بسیاری از مردم سوگوار شدند.

مـا هرگـز فرامـوش

برای دانلودهای رایگان ، روی عکس زیر کلیک / لمس کنید :