پیاده‌سازی یک شبکه ایمن و محافظت شده

چگونه یک اکسس‌پوینت مهمان را روی شبکه بی‌سیم خود فعال کنیم؟

به حکم ادب باید شبکه وای‌فای خود را در اختیار مهمانان قرار دهیم، اما این به آن معنا نیست که یک دسترسی باز و همه جانبه به کل شبکه را برای آنان فراهم کنیم. اگر نگران دسترسی سایرین به محتوای به اشتراک گذاشته روی شبکه خود هستید و می‌خواهید مهمانان شما فقط به اینترنت شبکه خانگی شما دسترسی داشته باشند، با ساخت یک نقطه دسترسی دوم روی روتر خود یک شبکه کاملا مجزا و محدود شده را در اختیار دوستان و اقوام خود قرار دهید.

چرا باید اکسس‌پوینت مهمان را روی شبکه بی‌سیم خود فعال کنیم؟

به دلایل متعددی شما باید شبکه خانگی خود را به گونه‌ای پیکربندی کنید تا دو نقطه دسترسی وای‌فای مجزا را در اختیار داشته باشید.

اصلی‌ترین دلیل که در مورد اغلب مردم و بیشتر کاربرها صدق می‌کند این است: شبکه خانگی خود را جداسازی می‌کنید تا مهمانان نتوانند به مسائل خصوصی شما دسترسی پیدا کنند. پیکربندی پیش فرض اغلب روترها یا **اکسس‌پوینت‌های** وای‌فای خانگی به شکلی است که از یک نقطه دسترسی بی‌سیم واحد استفاده می‌کند و هر کسی که مجوز دسترسی به این نقطه دسترسی بی‌سیم را داشته باشد، به تمام شبکه (چه باسیم چه بی‌سیم) متصل خواهد شد.

به عبارت دیگر، اگر شما به دوست، همسایه، مهمان یا هر شخص دیگری کلمه عبور شبکه وای‌فای خود را اعلام کنید، اجازه دسترسی به چاپگر شبکه، تمام محتوای به اشتراک گذاشته شده در این شبکه، دستگاه‌های ناامن درون شبکه و نظایر این را خواهید داد. شاید آن‌ها با اتصال به شبکه شما فقط می‌خواهند ایمیل‌های خود را چک کنند یا یک بازی آنلاین انجام دهند، اما شما با این کار این آزادی عمل را در اختیار آن‌ها قرار می‌دهید تا به هر کجایی از شبکه خانگی شما سرک بکشند.

هیچ یک از ما دوست هکری که انگیزه‌های مخرب داشته باشد، نداریم، اما این به معنای آن نیست که احتیاط نکنیم و مهمانان را همان جایی که باید باشند (دسترسی به اینترنت رایگان) باقی نگه نداریم.

یکی دیگر از دلایل راه‌اندازی **اکسس‌پوینت** با دو شناسه شبکه (SSID) این است که شما علاوه بر محدود کردن مکان دسترسی به شبکه زمان دسترسی را هم محدود کنید. برای مثال، اگر فرزند کوچکی در خانه دارید که نمی‌خواهید تا دیروقت مشغول گشت و گذار در اینترنت باشد می‌توانید کامپیوتر، موبایل یا تبلت آن‌ها را به **اکسس‌پوینت** دوم متصل کرده و آن را به‌گونه‌ای تنظیم کنید که مثلاً بعد از ساعت 9 شب دسترسی این SSID به اینترنت قطع شود.

به چه چیزی نیاز داریم؟

تمرکز این مقاله بر استفاده از یک روتر سازگار با DD-WRT است که امکان استفاده از دو SSID را فراهم می‌کند. همچنین به یک کپی از میان‌افزار DD-WRT نصب شده روی روتر نیاز خواهید داشت. این تنها راه برای تنظیم دو

SSID برای شبکه خانگی شما نیست. ما قصد داریم SSIDهای خود را روی روتر بی‌سیم معروف Linksys WRT54G پیاده‌سازی کنیم. اگر نمی‌خواهید زحمت نصب یک میان‌افزار (firmware) سفارشی را روی روتر قدیمی خود متحمل‌شده و تنظیمات اضافه را انجام دهید می‌توانید یک روتر جدیدتر مانند ASUS RT-N66U که از دو SSID پشتیبانی می‌کند، خریداری کنید یا یک روتر بی‌سیم دوم خریداری کنید و از آن به عنوان یک **اکسس‌پوینت** مستقل استفاده کنید. اما خوشایندتر خواهد بود تا همین سخت‌افزار موجود خود را (در این مقاله روتر بی‌سیم Linksys WRT54G) بهینه‌سازی کرده و از صرف هزینه‌اضافی جلوگیری کنید.

از کجا بدانم که روتر من سازگار است؟

برای تشخیص سازگاری روتر با قابلیت پیاده‌سازی راه‌اندازی **اکسس‌پوینت** با دو شناسه شبکه ابتدا باید بررسی کنید که آیا روتر مورد نظرتان از DD-WRT پشتیبانی می‌کند یا خیر؟ برای بررسی این موضوع می‌توانید به بانک اطلاعاتی روترهای DD-WRT به نشانی http://www.dd-wrt.com/site/support/router-database مراجعه کنید.
بعد از این‌که مطمئن شدید، روترتان با DD-WRT سازگار است، باید شماره اصلاحیه (Revision Number) تراشه روتر خود را بررسی کنید. برای مثال، اگر یک روتر لینک‌سیس خیلی قدیمی کارآمد دارید باید بدانید تراشه آن ممکن است از دو SSID پشتیبانی نکند.

مطلب پیشنهادی

توپولوژی‌های مختلف شبکه‌های بی‌سیم
انواع شبکه‌های بی‌سیم و نحوه استقرار آن‌ها

در شماره اصلاحیه تراشه روتر دو سطح از سازگاری وجود دارد. بعضی از روترها می‌توانند وظیفه پیاده‌سازی چند SSID را انجام دهند اما نمی‌توانند این SSIDها را منحصرا به نقاط دسترسی مجزا تقسیم کنند (برای نمونه یک آدرس مک مجزا برای هر SSID). در برخی مواقع این امر می‌تواند به مشکلاتی برای بعضی از دستگاه‌های وای‌فای منجر شود، زیرا آن‌ها نمی‌توانند تشخیص دهند که باید از کدام SSID استفاده کنند. شما می‌توانید با جست‌وجوی مدل روتر خود به همراه شماره نسخه چاپ شده در برچسب اطلاعات آن (این برچسب معمولا در زیر روتر چسبانده می‌شود) در گوگل شماره اصلاحیه آن را به دست آورید. اما گاهی اوقات اتفاق می‌افتد که این اطلاعات موجود در اینترنت درست نباشد. قابل اطمینان‌ترین روش برای بررسی شماره اصلاحیه تراشه داخلی روتر این است که خودتان اطلاعات آن را استخراج کنید. برای انجام این کار باید مراحل زیر را انجام دهید:
یک کلاینت Telnet باز کنید. این کار را هم می‌توانید از طریق نرم‌افزارهایی مانند PuTTY و هم فرمان Telnet خود ویندوز انجام دهید. سپس به آدرس آی‌پی روتر خود (معمولا 192.168.1.1) Telnet کنید. در مرحله بعد باید با استفاده از نام کاربری و کلمه عبور مدیریتی روتر خود لاگین کنید. توجه داشته باشید در برخی روترها به جای نام کاربری admin که در زمان ورود به صفحه تنظیمات تحت‌وب روتر وارد می‌کنید، از طریق Telnet باید نام کاربری را Root تایپ کنید.

بعد از این‌که به روتر خود لاگین کردید، فرمان زیر را در خط فرمان وارد کنید:

```
nvram show|grep corerev
```

خروجی این فرمان شماره اصلاحیه تراشه روتر را با فرمت زیر اعلام می‌کند:

```
wl0_corerev=9
wl_corerev=
```

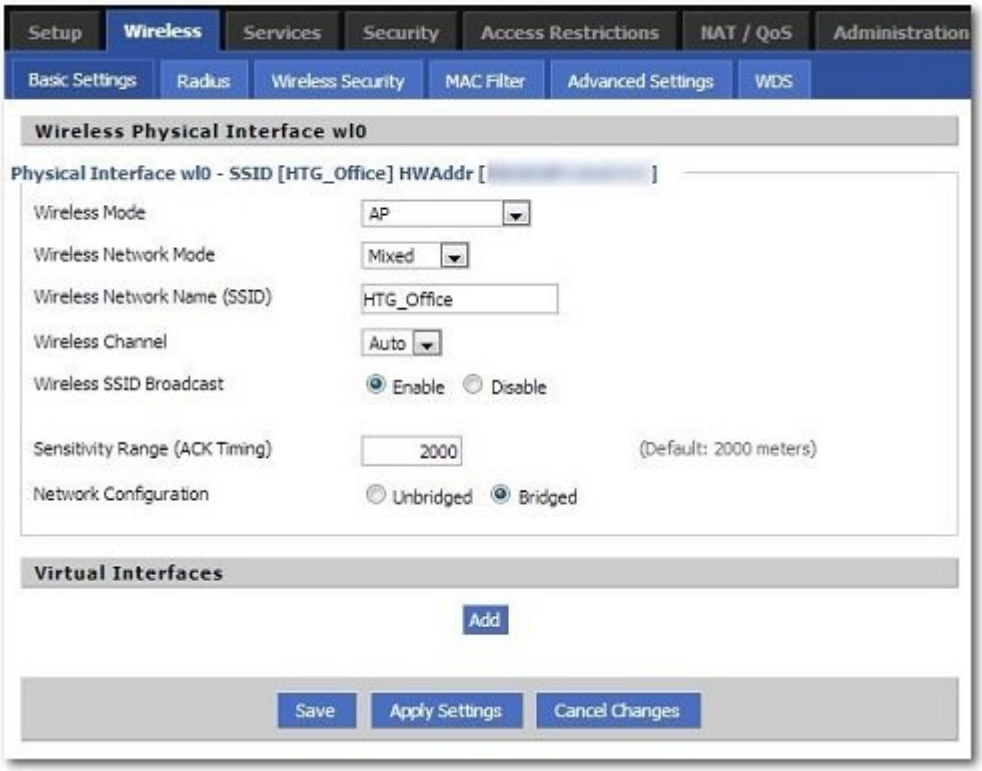
اطلاعات بالا به این معنا است که روتر ما یک رادیو دارد (wl0 نه wl1) و شماره اصلاحیه این تراشه رادیویی 9 است. اما این شماره چگونه به شما کمک می‌کند؟ شماره اصلاحیه که شما به دست می‌آورید، به این معنا است:

- 0 تا 4، یعنی این روتر از چند SSID پشتیبانی نمی‌کند. (چه با شناسه مستقل یا هر روش دیگری)
- 5 تا 8، یعنی این روتر از چند SSID پشتیبانی می‌کند. (اما نه با شناسه مستقل)
- 9 به بعد، یعنی این روتر از چند SSID پشتیبانی می‌کند. (با شناسه مستقل)

در مثال ما، تراشه روتر پایین‌ترین شماره اصلاحیه‌ای است که از چند SSID با شناسه‌های مستقل پشتیبانی می‌کند. بعد از این‌که متوجه شدید، روتر می‌تواند از چند SSID پشتیبانی کند باید میان‌افزار DD-WRT را روی آن نصب کنید. اگر روتر شما از DD-WRT استفاده می‌کند یا قبلا آن را نصب کرده‌اید، چه بهتر. اما اگر DD-WRT قبلا نصب نشده ما توصیه می‌کنیم نسخه مناسب روتر خود را از وب‌سایت DD-WRT دریافت و نصب کنید.

پیکربندی DD-WRT برای چند SSID

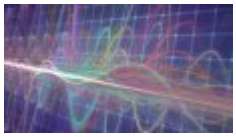
اکنون یک روتر سازگار دارید که DD-WRT روی آن نصب شده است. حالا زمان آن است که SSID دوم را برای آن تنظیم کنید. درست مانند زمان نصب یک میان‌افزار جدید که شما حتما باید از یک اتصال با سیم استفاده کنید، در اینجا ما به شما توصیه می‌کنیم که تنظیمات بی‌سیم خود را از طریق یک اتصال سیمی انجام دهید تا در زمان اعمال تغییرات یک اتصال بی‌سیم ارتباط شما با شبکه قطع نشود.



روی یک کامپیوتر که از طریق کابل اترنت به شبکه متصل شده مرورگر وب خود را باز کنید. به آدرس پیش‌فرض تنظیمات روتر (معمولا 198.168.1.1) وارد شوید. در رابط کاربری DD-WRT به بخش Wireless -> Basic Settings (نمایش داده شده در شکل بالا) بروید. مشاهده می‌کنید که شناسه SSID فعلی شبکه وای‌فای ما HTG_Office است. در پایین صفحه، در بخش Virtual Interfaces روی دکمه Add کلیک کنید. بخش خالی قبلی Virtual Interfaces با مشخصه‌های نمایش داده شده در شکل زیر گسترش پیدا خواهد کرد.

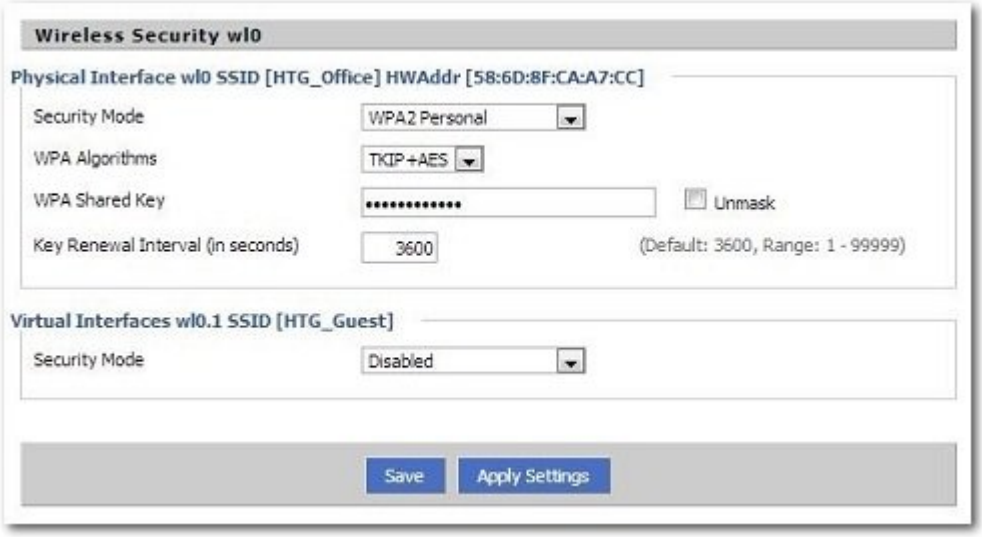
این رابط مجازی روی تراشه رادیویی فعلی‌تان سوار خواهد شد (به مشخصه wl0.1 در عنوان رابط مجازی توجه کنید). عبارت vap موجود در انتهای SSID پیش‌فرض نشان‌دهنده نقطه دسترسی مجازی (Virtual Access Point) است. شما می‌توانید این SSID را به هر نامی که مایل هستید تغییر دهید. برای راحتی کار و فراموش نکردن آن در موارد استفاده بعدی، در این مثال نام آن را به HTG_Guest تغییر می‌دهیم.
گزینه Wireless SSID Broadcast را روی حالت فعال باقی بگذارید. بسیاری از کامپیوترهای قدیمی‌تر و دستگاه‌های وای‌فای رابطه چندان خوبی با SSIDهای پنهان شده ندارند، چون یک شناسه مهمان مخفی شده نمی‌تواند برای یک شبکه مهمان مفید باشد.

مطلب پیشنهادی

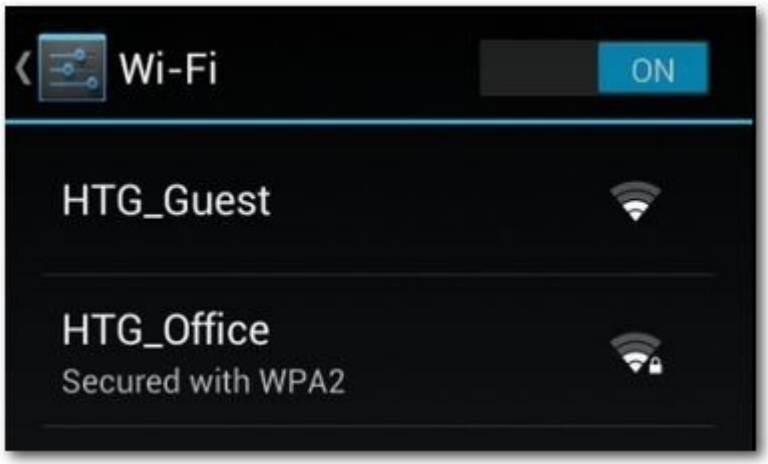


ورود امواج میلی‌متری به میدان
امواج میلی‌متری چگونه می‌توانند شبکه‌های بی‌سیم را متحول کنند؟

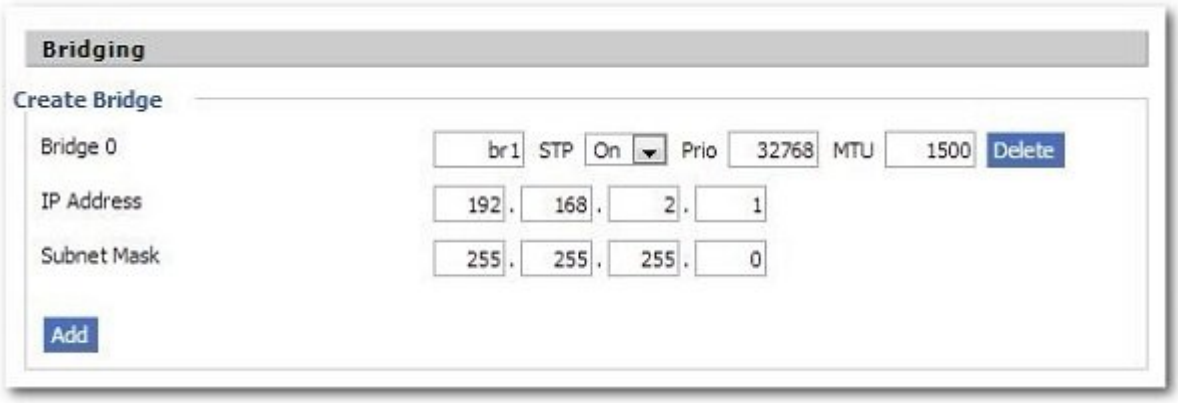
AP Isolation، یکی از تنظیمات امنیتی است که فعال یا غیرفعال بودن آن باید به صلاح‌دید خودتان انجام شود. اگر شما این گزینه را فعال کنید، هر کلاینتی که روی شبکه وای‌فای مهمان قرار دارد، به‌طور کامل از شبکه‌های دیگر جداسازی می‌شود. چنین اقدامی از لحاظ امنیتی بسیار مفید است، زیرا کاربران مخرب را از سایر کاربران دور نگه می‌دارد. اما چنین اقدامی بیشتر برای شبکه‌های سازمانی و هات اسپات‌های عمومی کاربرد دارد. در اغلب موارد استفاده خانگی و دفاتر تجاری کوچک دلیلی برای جداسازی نقاط دسترسی وجود ندارد.
گزینه Unbridged/Bridged در شبکه نشان‌دهنده آن است که آیا یک نقطه دسترسی وای‌فای باید به شبکه فیزیکی Bridged شود یا خیر. برخلاف روال معمول، باید این گزینه را روی حالت Bridged باقی بگذارید. در انتها بعد از این‌که SSID را تغییر دادید و سایر تنظیمات خود را اعمال کردید روی دکمه Save کلیک کنید.



در مرحله بعد به بخش Wireless -> Wireless Security می‌رویم:
به طور پیش فرض هیچ تنظیمات امنیتی روی نقطه دسترسی دوم اعمال نشده و برای آزمایش نقطه دسترسی دوم می‌توانید موقتا این تنظیمات را رها کنید تا به وارد کردن کلمه عبور روی دستگاه مورد آزمایش خود نیازی نداشته باشید. به هیچ‌وجه توصیه نمی‌شود برای همیشه این تنظیمات را دست نخورده و شبکه را باز رها کنید. تفاوتی ندارد که تنظیمات امنیتی را اعمال کنید یا آن‌ها را دست نخورده باقی بگذارید در هر صورت باید روی دکمه Save و Apply Settings کلیک کنید تا تنظیماتی را که در هر دو قسمت قبل اعمال کردیم ذخیره و آماده کار شود. توجه داشته باشید، اعمال این تغییرات نزدیک به دو دقیقه طول خواهد کشید.
حالا زمان آن رسیده تا ببینیم دستگاه‌های موجود در منطقه تحت پوشش امواج این شبکه می‌توانند هر دو نقطه دسترسی اولیه و ثانویه را شناسایی کنند. روی تلفن هوشمند خود به بخش تنظیمات Wi-Fi بروید و ببینید چه شبکه‌هایی را شناسایی می‌کند. شکل زیر صفحه تنظیمات Wi-Fi یک گوشی اندروید را نشان می‌دهد:

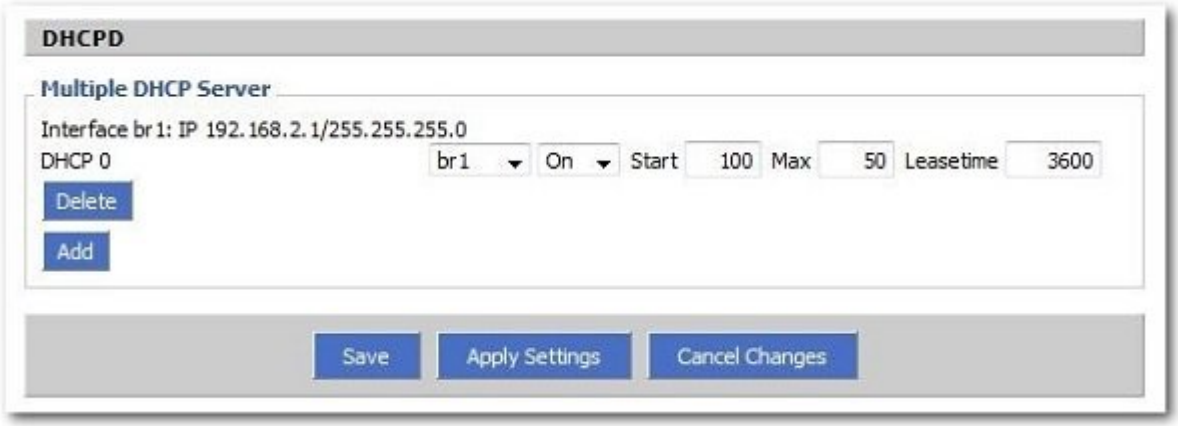


ما هنوز نمی‌توانیم به نقطه دسترسی دوم متصل شویم و باید چند تغییر دیگر را روی روتر اعمال کنیم. اما نمایش داده شدن هر دو نام در فهرست اسامی وای‌فای نشان‌دهنده آن است که ما تا این جای کار درست عمل کرده‌ایم.
مرحله بعدی کار، فرآیند جداسازی این SSIDها از طریق اختصاص دادن طیفی از آدرس‌های آی‌پی مستقل به دستگاه‌های وای‌فای مهمان خواهد بود. به بخش Setup -> Networking بروید. زیر قسمت Bridging روی دکمه Add کلیک کنید.

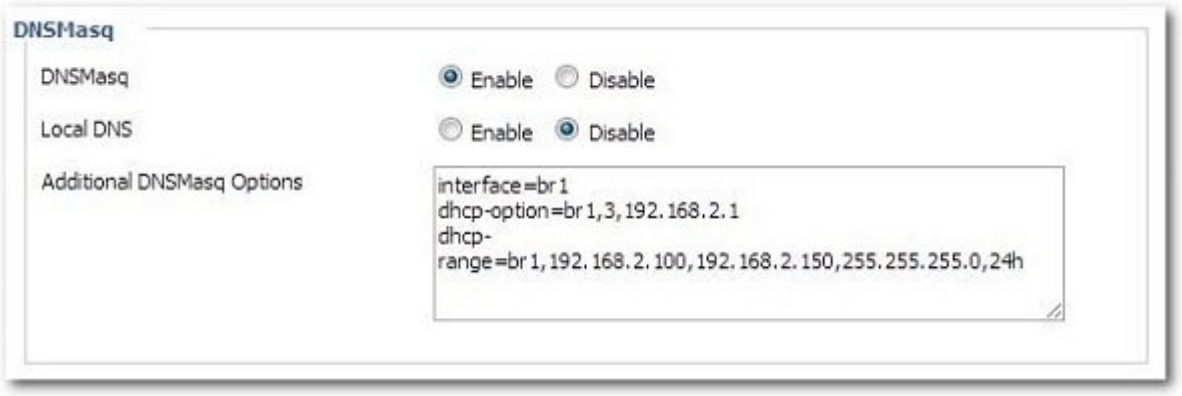


ابتدا اسلات اولیه را به br1 تغییر دهید و باقی مقادیر را دست‌نخور ده رها کنید. در این مرحله نمی‌توانید ورودی‌های IP/Subnet نمایش داده شده در شکل بالا را ببینید. روی Apply Settings کلیک کنید. این پل جدید در بخش Bridging با بخش‌های موجود IP و Subnet قرار خواهد گرفت. مقدار آدرس آی‌پی را به ترتیب بعد از آی‌پی شبکه تعیین کنید. به‌عنوان مثال، اگر آدرس آی‌پی شبکه اصلی شما 192.168.1.1 است، این آدرس را 192.168.2.1 قرار دهید . مقدار Subnet Mask را 255.255.255.0 تعیین کنید و یک بار دیگر روی Apply Settings کلیک کنید.

در قسمت Assign to Bridge روی دکمه Add کلیک کنید. Bridge جدیدی را که قبلا ایجاد کرده بودید، انتخاب کرده و آن را با رابط wl0.1 جفت کنید، سپس روی دکمه Save و Apply Settings کلیک کنید.
بعد از این‌که تغییرات اعمال شد، به پایین صفحه حرکت کرده و بخش DHCPD را پیدا کنید. در این بخش روی دکمه Add کلیک کنید. اسلات اولیه را به br1 تغییر دهید و باقی مقادیر را همانند شکل زیر دست نخورده رها کنید.



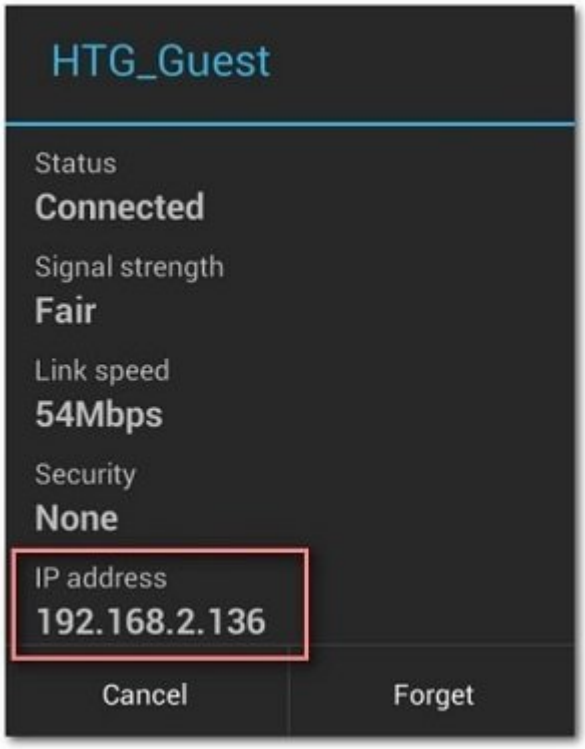
یک بار دیگر روی دکمه Apply Settings کلیک کنید. بعد از اتمام کار صفحه Setup -> Networking باید به سراغ تنظیمات DHCP بروید. در این مرحله به بخش Services بروید.



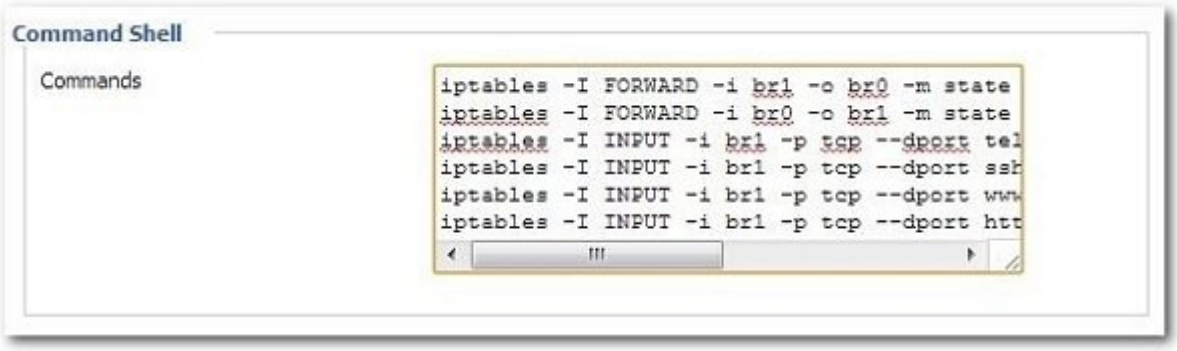
در قسمت Services باید مقداری از کد را به بخش DNSMasq اضافه کنیم تا روتر آدرس‌های آی‌پی پویا را به دستگاه‌های متصل شده به شبکه مهمان اختصاص دهد. به بخش DNSMasq بروید. در کادر Additional DNSMasq Options کد زیر را وارد کنید:

```
# Enables DHCP on br1
interface=br1
# Set the default gateway for br1 clients
dhcp-option=br1,3,192.168.2.1
# Set the DHCP range and default lease time of 24 hours for br1 clients
dhcp-range=br1,192.168.2.100,192.168.2.150,255.255.255.0,24h
```

حالا روی دکمه Apply Settings کلیک کنید.
بعد از متصل شدن به SSID مهمان، آدرس آی‌پی را بررسی کنید. شما باید یک آی‌پی در محدوده‌ای که در بالا تعیین کردیم، داشته باشید. در اینجا به راحتی از طریق تلفن هوشمند خود می‌توانید این موضوع را بررسی کنید:



تا اینجا همه چیز خوب به نظر می‌رسد، نقطه دسترسی دوم ما یک آدرس آی‌پی پویا در محدوده مشخص شده دریافت کرده و مهمان شما حالا می‌تواند به اینترنت دسترسی داشته باشد. تنها مشکل اینجا است که نقطه دسترسی دوم هنوز به منابع شبکه اصلی دسترسی دارد. این به معنای آن است که تمام منابع موجود در شبکه مانند چاپگر و پوشه‌های به اشتراک گذاشته شده همچنان برای شبکه مهمان قابل مشاهده است.
اگر می‌خواهید دسترسی شبکه مهمان را به این منابع محدود کنید باید لینک نقطه دسترسی دوم را به شبکه فیزیکی قطع کنید.



به بخش Administration -> Commands بروید. یک ناحیه با نام Command Shell را مشاهده می‌کنید. فرامین زیر را بدون خط‌های توضیح # در کادر Commands وارد کنید.

```
#Removes guest access to physical network
iptables -I FORWARD -i br1 -o br0 -m state --state NEW -j DROP
iptables -I FORWARD -i br0 -o br1 -m state --state NEW -j DROP
#Removes guest access to the router’s config GUI/ports
iptables -I INPUT -i br1 -p tcp --dport telnet -j REJECT --reject-with tcp-reset
iptables -I INPUT -i br1 -p tcp --dport ssh -j REJECT --reject-with tcp-reset
iptables -I INPUT -i br1 -p tcp --dport www -j REJECT --reject-with tcp-reset
iptables -I INPUT -i br1 -p tcp --dport https -j REJECT --reject-with tcp-reset
```

روی دکمه Save Firewall کلیک کرده و یک بار روتر خود را ریبوت کنید.
این قوانین فایروال اضافی همه چیز را روی این دو Bridges (شبکه خصوصی و شبکه عمومی/مهمان) از گفت‌وگو و رد کردن اتصال بین یک کلاینت شبکه مهمان و telnet, SSH تا پورت‌های سرور وب روی روتر متوقف می‌کند

تاریخ انتشار:
22 مرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/tricks/network-tricks/15907/%DA%86%DA%AF%D9%88%D9%86%D9%87-%DB%8C%DA%A9-%D8%A7%DA%A9%D8%B3%D8%B3%E2%80%8C%D9%BE%D9%88%DB%8C%D9%86%D8%AA-%D9%85%D9%87%D9%85%D8%A7%D9%86-%D8%B1%D8%A7-%D8%B1%D9%88%DB%8C-%D8%B4%D8%A8%DA%A9%D9%87-%D8%A8%DB%8C%E2%80%8C%D8%B3%DB%8C%D9%85-%D8%AE%D9%88%D8%AF-%D9%81%D8%B9%D8%A7%D9%84-%DA%A9%D9%86%DB%8C%D9%85%D8%9F