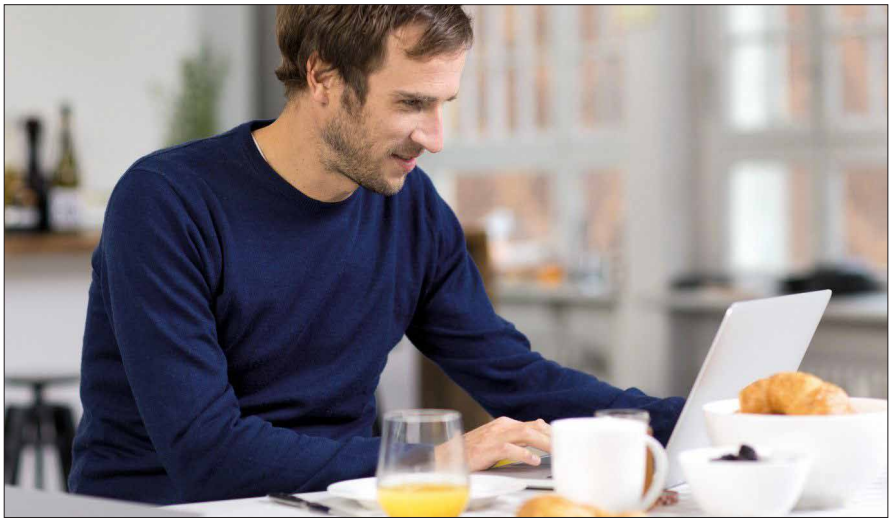
5 GHz, Bandsteering & Co.

WLAN-Tipps im Praxis-Check

Viele WLAN-Empfehlungen versprechen, Ihr Netzwerk schneller und sicher zu machen. Doch nicht jeder Tipp passt für jedes Netzwerk. Wir checken die populärsten Aussagen und sagen Ihnen, was Sie tun müssen, damit sie Ihnen tatsächlich helfen.

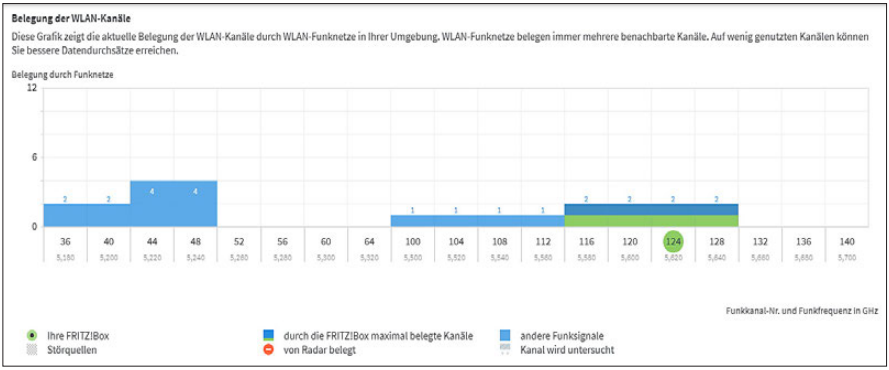


› Fritzbox: Neue Funktionen für schnelleres WLAN (Foto: AVM)

Über WLAN scheint schon alles gesagt: Unzählige Tipps erklären Ihnen, wie Sie das Funknetz schneller und sicherer machen. Und theoretisch sind sie auch alle richtig. Allerdings kommt es beim WLAN vor allem auf die Praxis an – und die unterschiedet sich von Funknetz zu Funknetz: Ob ein Tipp hilft, hängt davon ab, wie viele Geräte mit welchem WLAN-Standard arbeiten, welchen Bereich das WLAN abdecken soll und welchen Störungen es ausgesetzt ist. Es kann sein, dass Sie mit WLAN-Tipps sehr zufrieden sind, weil Sie damit Tempo und Reichweite verbessern, ein Bekannter Ihnen aber ganz andere Vorschläge macht, weil sie in seinem Funknetz gut funktioniert haben.

Aus diesem Grund überprüfen wir häufig genannte WLAN-Empfehlungen für Tempo und Sicherheit. Alle haben Vor- und Nachteile, die sie ideal für ein Netzwerk machen können, während sie zu einem anderen weniger gut passen. So können Sie selbst entscheiden, welche Maßnahmen Sie nutzen oder für Ihre Situation anpassen wollen.

Tempo: Ist 5 GHz immer die schnellere Frequenz?



› Nicht immer ist die 5-GHz-Frequenz die bessere Lösung: Auch dort können sich WLANs gegenseitig stören – vor allem, wenn Router oder Clients nicht die höheren Kanäle ab 52 nutzen dürfen.

Seit es WLAN-Geräte mit Dual-Band-Unterstützung gibt, die über 2,4 und über 5 Ghz übertragen, lautet die Empfehlung: Nutzen Sie für höheres Tempo unbedingt die 5-GHz-Frequenz. Das ist natürlich nicht falsch: Über 5 GHz können Router, Repeater und Clients breitere Funkkanäle nutzen, was eine höhere Übertragungsrate ermöglicht. Außerdem steht über 5 GHz ein deutlich größeres Frequenzspektrum für WLAN zur Verfügung – 455 MHz gegenüber 83,5 MHz bei der 2,4-GHz-Frequenz. Das bedeutet mehr überlappungsfreie Kanäle, weshalb mehr unterschiedliche Funknetze über diese Frequenz übertragen können, ohne sich gegenseitig zu stören. Zudem dürfen Geräte über 5 GHz eine höhere Strahlungsleistung nutzen – je nach Kanal 200 mW oder 1 Watt –, während über 2,4 GHz nur maximal 100 mW erlaubt sind. Das sorgt in der Praxis auch meist für eine vergleichbare Reichweite, obwohl Funkwellen auf der 5-GHZ-Frequenz grundsätzlich eine höhere Dämpfung erfahren.

Abhängig von den Bedingungen bei Ihnen kann das Reichweitenproblem aber auch ein wichtiges Argument gegen 5 GHz sein: Muss das WLAN-Signal viele Wänden und Decken durchqueren, kann sich das Tempo so stark reduzieren, dass eine Verbindung über 2,4 GHz die bessere Lösung ist. Zudem lassen sich mit einigen Dual-Band-Geräten die meisten 5-GHz-Kanäle gar nicht nutzen: Beherrschen Router oder Client die Funktion DFS (Dynamic Frequency Selection) nicht, dürfen sie nur über die unteren Kanäle 36 bis 48 funken. In diesem Fall lässt sich ausschließlich ein einziger 80 MHz breiter Funkkanal nutzen, und Ihr WLAN kann anderen Funknetzen in der Nachbarschaft, die ebenfalls über diesen Kanal übertragen, nicht ausweichen. In der Folge verringert sich das Übertragungstempo, weil die Netzwerke aufeinander warten müssen.

Versteht der Router DFS, aber einige Clients nicht, kommen diese gar nicht ins WLAN, wenn die Basisstation einen Kanal über 48 nutzt. Dann müssen Sie einen Kanal darunter fest im Router einstellen, mit den erwähnten Konsequenzen für das Tempo.

Fazit: In den meisten Fällen ist die Übertragung über 5 GHz schneller. Denn fast überall sind immer noch mehr WLAN-Geräte über 2,4 als über 5 GHz unterwegs, sodass selbst eine nicht optimale Transferrate über 5 GHz deutlich besser ist als der Datenaustausch über 2,4 GHz.

Bei Problemen mit Geräten ohne DFS sollten Sie über deren Austausch nachdenken, damit Sie die Tempovorteile von 5 GHz tatsächlich nutzen können.

Band-Steering: Gleiche SSID für alle WLANs nutzen?

› Nur bei gleicher SSID funktionieren Tempofunktionen wie Band-Steering: Ob Ihre WLAN-Clients damit zurechtkommen, lässt sich in einer Fritzbox zum Beispiel im Ereignis-Protokoll nachprüfen.

Aktuelle WLAN-Router versprechen, per Band-Steering das Tempo für alle Geräte zu erhöhen: Mit dieser Funktion können sie WLAN-Clients optimal auf die Frequenzen verteilen, sodass sie sich nicht stören und immer die beste Verbindung haben. Dafür müssen die WLANs über 2,4 und 5 GHz dieselbe Netzwerkkennung (SSID) haben. Nur dann kann der Router die Clients ohne eine längere Pause umleiten.

Allerdings überlassen Sie dann dem Router komplett die WLAN-Verwaltung – manuell eingreifen können Sie nicht mehr. Außerdem bleibt meist unklar, nach welchen Regeln er die Clients verteilt. Nur in wenigen Routern für Privatkunden können Anwender nämlich detaillierte Anweisungen für das Band-Steering eintragen, um zum Beispiel festzulegen, dass Clients bei einer bestimmten Datenrate oder Signalstärke die Frequenz ändern sollen.

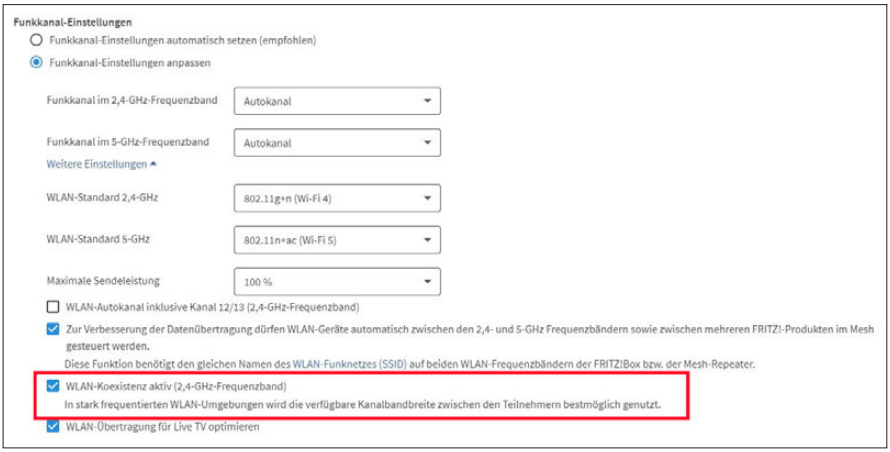
In der Praxis kann das dazu führen, dass einige WLAN-Clients zu spät oder gar nicht zwischen 2,4 und 5 GHz wechseln: Dann arbeiten sie langsamer, als wenn Sie sie manuell auf die bessere Frequenz festlegen und bremsen schnellere Geräte aus. Um von Band-Steering zu profitieren, sollten Sie daher dafür sorgen, dass

alle WLAN-Geräte immer mit einer aktuellen Firmware und den neuesten Treibern laufen. Bei Clients achten Sie darauf, dass sie die WLAN-Standards 802.11k und 802.11v unterstützen, die Band-Steering verbessern.

Haben Sie bei bestimmten Geräten den Verdacht, dass sie mit Band-Steering nicht zurechtkommen, können Sie zum Beispiel im Ereignisprotokoll des Routers prüfen, ob er diese Clients umleitet oder ob sie permanent auf derselben Frequenz unterwegs sind, selbst wenn sie sich vom Router entfernen. Wenn Band-Steering funktioniert, steht dann zum Beispiel bei einer Fritzbox unter „System –› Ereignisse" ein Eintrag wie „WLAN-Gerät wurde umgemeldet (Band-Steering): Automatischer WLAN-Bandwechsel zur verbesserten Datenübertragung".

Fazit: Je aktueller die Geräte in Ihrem WLAN sind, desto höher sind die Chancen, dass Band-Steering einen Tempovorteil bringt. Wollen Sie sich auf diese Funktion nicht verlassen, müssen Sie für jedes WLAN-Band eine eigene SSID festlegen und die Geräte anschließend manuell verbinden. Dieser Aufwand lohnt sich, wenn Sie auf diese Weise vor allem stationäre Geräte wie PC oder Fernseher ins Funknetz bringen und sich die Zahl der aktiven Clients in Ihrem Funknetz nicht ändert.

WLAN-Koexistenz abschalten für mehr Tempo?



› Die Option „WLAN-Koexistenz" soll dafür sorgen, dass verschiedene WLANs im meist überfüllten 2,4-GHz-Band ausreichend Platz haben. Wenn Sie sie abschalten, können Sie aber das Tempo erhöhen.

Viele Router bieten für 2,4 GHz eine Einstellung wie „WLAN-Koexistenz aktiv" oder „20/40 MHz Koexistenz". In vielen WLAN-Foren wird darüber debattiert, ob der

Router diese Funktion nutzen sollte oder nicht. Grundsätzlich bringt es Ihnen mehr Tempo, wenn Sie diese Option abschalten: Dann nutzt der Router über 2,4 GHz auf jeden Fall breitere 40-MHz-Funkkanäle und kann Daten schneller übertragen, sofern auch die WLAN-Clients diese Kanalbandbreite unterstützen. Haben Sie allerdings keine entsprechenden Geräte, bringt das Abschalten der Option keine Vorteile.

Arbeiten aber in der Nachbarschaft weitere WLANs, stört Ihr Router diese massiv, wenn die Option deaktiviert ist, beziehungsweise der Nachbarrouter mit ausgeschalteter Koexistenz beeinflusst Ihr WLAN negativ. Diesen Kampf um die Vorherrschaft im Funkkanal soll die Koexistenz-Funktion vermeiden: Ist sie aktiv, arbeitet Ihr Router mit einem 40-MHz-Kanal, bis er ein anderes Netzwerk auf 2,4 GHz entdeckt. Dann schaltet er auf 20 MHz, damit jedes WLAN möglichst störungsfrei arbeiten kann.

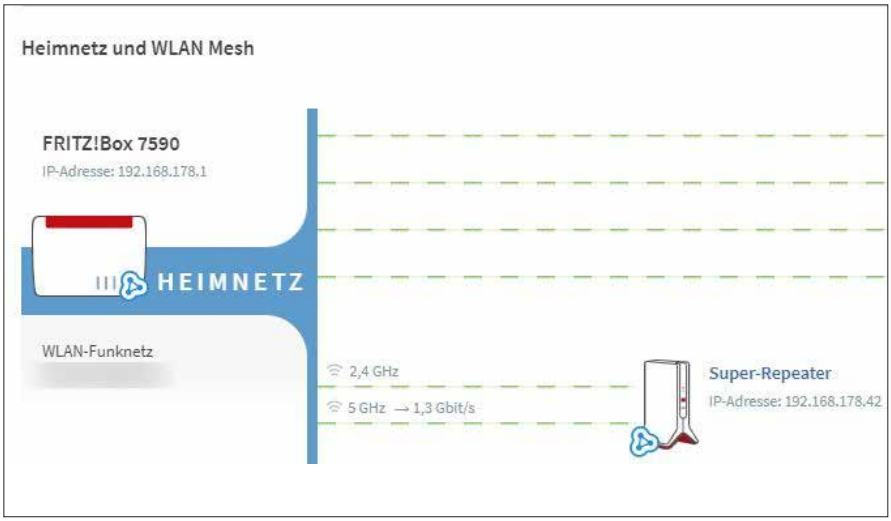
Fazit: Mit dieser Option entscheiden Sie, ob Sie unter allen Umständen Tempo oder lieber ein netter Nachbar sein wollen. Funkt Ihr WLAN allein auf weiter Flur, spricht nichts dagegen, die Koexistenz auszuschalten. Haben Sie nur ein WLAN in der Nachbarschaft, können Sie eine Absprache zum beiderseitigen Vorteil treffen: Ihr Nachbar und Sie aktivieren im jeweiligen Router über 2,4 GHz die Kanäle 12 und 13. Anschließend setzt der eine sein WLAN auf Kanal 1, der andere seins auf Kanal 13. Dann können beide Funknetze mit 40-MHz-Kanälen arbeiten, ohne sich gegenseitig zu stören.

Ein anderer Weg, hohe Transferraten und Nachbarschaftsfrieden zu verbinden: Reduzieren Sie die Sendeleistung des Routers, damit seine Signale die Nachbar-WLANs nicht mehr erreichen.

Router und Repeater vom selben Hersteller kaufen?

Netzwerkhersteller wollen Ihnen gerne so viele Geräte wie möglich verkaufen: Deshalb betonen sie, dass sich WLAN-Router und -Repeater besonders einfach einsetzen lassen, wenn sie aus einer Hand stammen. Auf das Übertragungstempo hat es aber keinen Einfluss, ob Router und Router von einem Hersteller kommen. Wichtiger für einen schnellen Datentransfer ist, dass sie den gleichen WLAN-Standard nutzen und die Zahl der unterstützen WLAN-Frequenzen sowie der MIMO-Streams zusammenpassen. So sollten Sie etwa keinen Dual-Band-Router mit einem Single-Band-Repeater koppeln, wenn es schnell gehen soll.

Wollen Sie Router und Repeater in einem Mesh zusammenfassen, müssen Sie beim selben Hersteller bleiben: Denn für WLAN-Mesh gibt es keinen herstellerunabhängigen Standard beziehungsweise verschiedene Hersteller verstehen darun-



› Am blauen Symbol bei Router und Repeater sehen Sie bei Fritz-Produkten, dass sich beide Geräte im gemeinsamen Mesh befinden und über ein Menü gesteuert werden können.

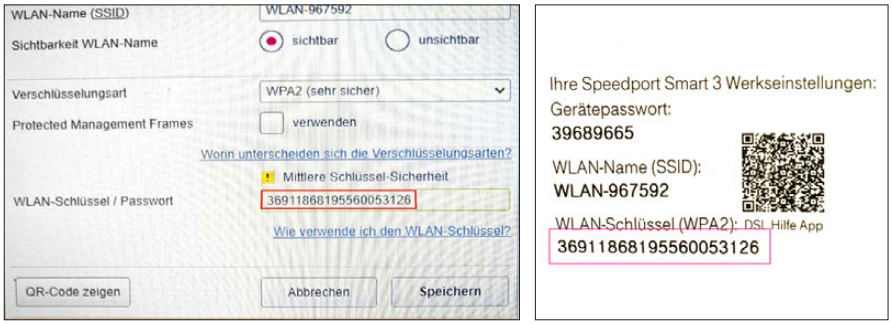
ter unterschiedliche Funktionen. Deshalb lassen sich auch nur Geräte von einem Hersteller in einem Mesh-Netzwerk kombinieren – bei der Fritzbox zum Beispiel nur Fritz-Repeater und Fritz-Powerline-Adapter. Nur auf diese Weise können Sie Mesh-Vorteile wie APSteering nutzen oder Einstellungen, die für alle Geräte gelten sollen, im Menü eines einzigen Mesh-Knotens vornehmen.

Fazit: Auch ohne Mesh ist es fürs Einrichten und Bedienen von Router und Repeater einfacher, bei einem Hersteller zu bleiben: Die Geräte haben oft ein sehr ähnliches Menü, sodass Sie sich schnell zurechtfinden.

Müssen Sie das WLAN-Passwort regelmäßig ändern?

Wenn Ihr WLAN-Passwort sicher ist, sollten Sie es nicht ändern. Sicher bedeutet, dass der Aufwand für einen Angreifer, es herauszufinden zu hoch ist: Das sollte bei einem Passwort mit zehn Zeichen der Fall sein, sofern es in keinem Wörterbuch zu finden ist und nichts mit Ihnen zu tun hat.

Aber mindestens einmal sollten Sie das WLAN-Passwort auf jeden Fall ändern: Denn alle WLAN-Router werden inzwischen mit einem voreingestellten WLAN-Schlüssel verkauft – und der ist irgendwo hinterlegt: Entweder steht er auf dem Router-Gehäuse oder auf einem Zettel, der mit dem Router kam. Sie können also nicht ausschließen, dass dieses Passwort unbekannt bleibt. In diesem Zusam-



› Auf jeden Fall sollten Sie das WLAN-Passwort ändern, mit dem der Router verkauft wird. Es ist nämlich auf dem Gehäuse oder auf einer mitgelieferten Karte aufgedruckt.

menhang sollten Sie auch darüber nachdenken, ob Sie das Passwort nicht schon einmal jemandem mitgeteilt haben – etwa einem Gast, weil der schnell ins Internet musste oder Ihren Freunden im Rahmen einer Feier. In diesem Fall ist der Wechsel des WLAN-Schlüssels angeraten.

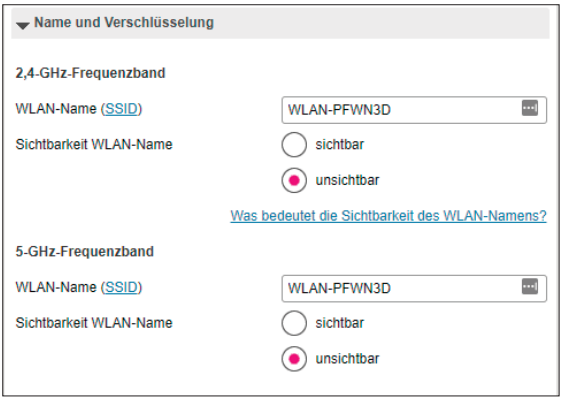
Fazit: Haben Sie einmal ein ausreichend starkes WLAN-Passwort erstellt, müssen Sie es nicht mehr ändern.

Sollten Sie Ihr Netzwerk unsichtbar machen?

Auf den ersten Blick eine einleuchtende Empfehlung: Stellen Sie den Router so ein, dass er die Netzwerkkennung (SSID) Ihre WLANs verbirgt – was ein Angreifer nicht sieht, kann er nicht attackieren.

Allerdings verstecken Sie Ihr Funknetz damit nicht wirklich. Die meisten Analyse-Tools zeigen das namenlose WLAN an und Windows erkennt es bei den verfügbaren WLANs als „Ausgeblendetes Netzwerk". Denn die SSID taucht bei der Datenübertragung immer noch auf – mit der Verstecken-Option verhindern Sie nur, dass der Router die WLAN-Kennung automatisch aussendet, damit Clients ihn finden können. Doch das WLAN ist weiterhin vorhanden, und deshalb antwortet der Router zum Beispiel bekannten Clients, die bei ihrer Verbindungsanfrage die SSID im Klartext aussenden.

Ein Angreifer muss technisch nicht besonders versiert sein, um zu entdecken, was Sie verbergen wollen – und möglicherweise macht gerade das eine Attacke attraktiver. Auch wenn Sie ein neues Gerät im WLAN anmelden wollen, erschwert die versteckte SSID die Verbindung, weil Sie ihm nicht nur das WLAN-Passwort, sondern zuvor auch die SSID mitteilen müssen.



› Über eine Einstellung im Menü weisen Sie den Router an, die Netzwerkkennung nicht mehr bekannt zu geben. Das WLAN wird dadurch aber nicht unsichtbar – Angreifer können es trotzdem entdecken.

Sinnvoll ist eine versteckte SSID, wenn Sie in der Firma oder zu Hause Besucher in das für sie vorgesehene WLAN leiten wollen: Aktivieren Sie das Gast-WLAN und verstecken Sie die SSID Ihres Haupt-WLANs, damit niemand versucht, sich mit dem anderen Netzwerk zu verbinden.

Fazit: Die SSID zu verstecken schützt gegen zufällige Verbindungsversuche, nicht gegen gezielte Angriffe. Es erhöht die Netzwerk-Sicherheit minimal – und nur dann, wenn Sie zudem andere, sinnvollere Maßnahmen einsetzen wie ein starkes WLAN-Passwort.

Wie beim SSID-Verstecken geht es auch bei Zugangsbeschränkungen per MAC-Adresse um die Frage: Bringt die Maßnahme mehr Sicherheit, als sie Aufwand verursacht?

WLAN per MAC-Filter für unbekannte Geräte sperren?

Per MAC-Filter legen Sie fest, dass nur Geräte ins WLAN kommen, die der Router kennt. Er identifiziert sie anhand der MAC-Adresse, die für jedes Geräte eigentlich einzigartig ist. Diese Methode nutzt der Router zum Beispiel bei einer Kindersicherung oder bei Zeitbeschränkungen einzelner Geräte für den Onlinezugang.

Allerdings meldet nicht die WLAN-Hardware direkt ihre MAC-Adresse an den Router, sondern das Betriebssystem: Da diese Übertragung unverschlüsselt passiert, lässt sich die MAC-Adresse verändern: Dafür gibt es zahlreiche Tools im Internet. Das nutzt der Nachwuchs, um einem per Kindersicherung gesperrten Gerät eine neue MAC-Adresse zu verpassen, woraufhin der Router ihm als neuem Client unbeschränkten Zugang erlaubt. Haben Sie alle unbekannten Geräte ausgesperrt, muss der Eindringling die MAC-Adresse eines erlaubten Gerätes kennen, um den Filter auszutricksen.