Handbuch für Hotspot-Router mit Firmware 3.0

Stand der Firmware: hotsplotsWrt-3.0-039
Stand: 09.12.2011

Inhaltsverzeichnis

Einleitung

Dieses Handbuch erläutert die Einrichtung eines WLAN-Hotspots mit einem WLAN-Router bzw. die Erweiterung eines WLAN-Hotspots durch Access Points oder Repeater. Voraussetzung ist ein Gerät, für das eine spezielle Firmware von HOTSPLOTS vorliegt. Das Handbuch behandelt zur Zeit folgende Hardware:

- TP-LINK TL-WR1043ND
- NETGEAR WNDR3700 v1 und v2 (Im v3 ist vollkommen andere Hardware verbaut, die nicht von HOTSPLOTS unterstützt wird.)

Wesentliche Änderungen in der Firmware-Version 3.0

Die Firmware-Generation 3.0 unterstützt leistungsfähigere Hardware. Im Vergleich zur alten Firmware 2.0 ergeben sich folgende Änderungen:

- Das Webinterface ist nur noch über Port 8080 erreichbar.
- Der VPN-Tunnel zu den HOTSPLOTS-Servern wird in jedem Fall aufgebaut. Zu Wartungszwecken können sich Mitarbeiter auf dem Hotspot einloggen, wenn ihnen das Passwort bekannt ist.
- Bei eingeschaltetem VPN-Routing wird nur noch der Hotspot-Traffic über unsere VPN-Server geroutet. Privater Traffic am LAN-Port des Hotspots, oder Traffic, der vom Hotspot selbst erzeugt wird, wie z.B. das Pulssignal oder Funktionen zur Synchronisation der Uhrzeit, wird über die Default-Route des Hotspots geleitet.
- Eine Firewall verhindert, dass Hotspot-Traffic bei eingeschaltetem VPN-Routing direkt ins Internet gelangt. Bei kurzzeitigen Unterbrechungen des VPN-Routings (z.B. bei einer DSL-Wiedereinwahl des Hotspots) wird der Hotspot-Traffic unterbrochen.
- In Werkseinstellung wird jeglicher Hotspot-Traffic in Richtung lokal angeschlossener Netze unterdrückt. Sollen Hotspot-Clients z.B. lokal angeschlossene Drucker verwenden dürfen, können dafür Ausnahmeregeln angegeben werden.
- Über das Pulssignal kann der Hotspot von den HOTSPLOTS-Servern zu einem automatischen Update veranlasst werden. Updates können individuell für jeden einzelnen Hotspot zur Verfügung gestellt werden.
- Im Administrations-Menü ist per Default eine Option eingeschaltet, die dazu führt, dass die Systemeinstellungen des Hotspots automatisch an HOTSPLOTS übertragen werden. Dies erleichtert den Support und im Falle eines Gerätetausches kann HOTSPLOTS identisch konfigurierte Geräte verschicken.
- Aufgrund der neuen Hardwaregeneration ist ein gemischter WDS-Betrieb mit alter Hardware nur eingeschränkt möglich: Die neue Generation kann als Repeater für alte Geräte wie den Linksys WRT54GL oder Buffalo WHR-HP-G54 eingesetzt werden, aber nicht umgekehrt.
- Faire Bandbreitenkontrolle. Bei aktivierter Bandbreitenkontrolle kann vorgegeben werden, welche Bandbreite den Hotspot-Clients zur Verfügung gestellt werden soll. Zusätzlich misst der Hotspot im Stundenintervall die zur Verfügung stehende Gesamtbandbreite und justiert die Bandbreitenkontrolle automatisch. Bei aktivierter Option wird die Bandbreite fair auf alle Hotspot-Clients aufgeteilt. Einzelne Nutzer können mit mehreren parallelen Downloads nichts überproportional viel Bandbreite abgreifen.
  Hinweis: Bis Version 3.0-039 gab es einen Fehler bei der automatischen Bandbreitenbestimmung, der dazu führen konnte, dass die Gesamtbandbreite mit der Zeit nicht voll ausgeschöpft wurde.
- mssfix-Option für VPN-Routing auswählbar: In seltenen Fällen können alte DSL-Modems oder exotische Internetanbindungen die MTU-Größe negativ beeinflussen. Mit der Aktivierung der neuen Option läuft das VPN-Routing auch unter diesen Bedingungen stabil.

1 Installation der Firmware

1.1 TP-LINK TL-WR1043ND

Der Router kann über das Web-Interface der Original-Firmware mit der Firmware von HOTSPLOTS geflasht werden:

1. Starten Sie einen Webbrowser und verbinden Sie ihn mit dem Router, so wie in dessen Bedienungsanleitung beschrieben. Es ist nicht erforderlich, Software von der mitgelieferten CD zu installieren, auch wenn dies als Hinweis vermerkt ist.
2. Wählen Sie dann die Seite ***„System-Tools – Firmware Upgrade“***.

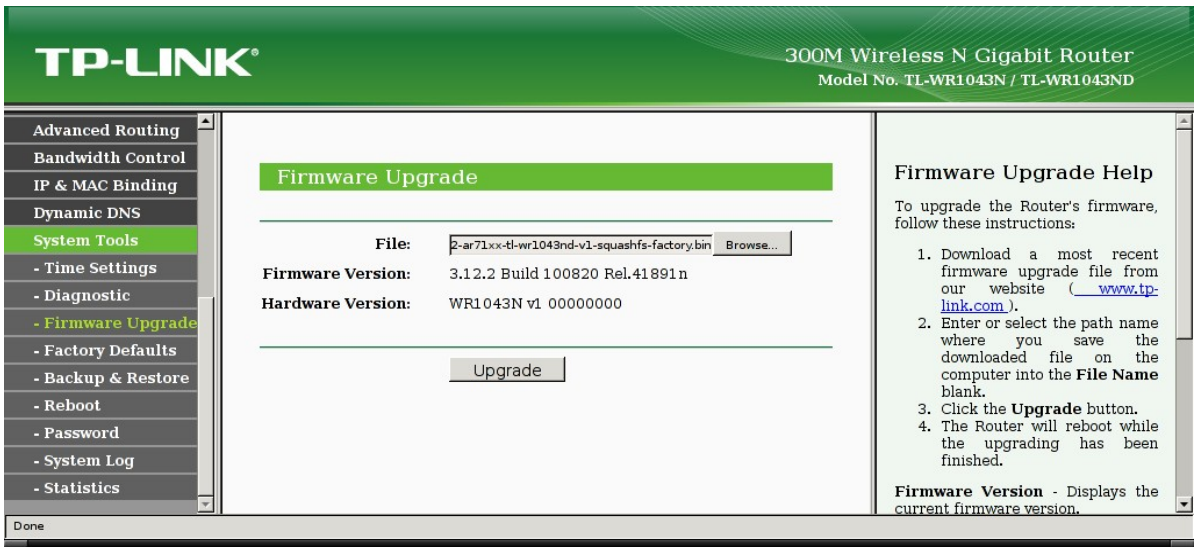


Abbildung 1: Das Webinterface der Original-Firmware von TP-Link zum Upgrade auf die Firmware von HOTSPLOTS

3. Wählen Sie als Datei ein Firmware-Image von HOTSPLOTS aus:
   hotsplotsWrt-3.0-xxx-ar71xx-tl-wr1043nd-v1-squashfs-factory.bin
   Achten Sie dabei auf den Namensteil „factory“!

4. Führen sie nun das Upgrade aus. Nach dem Installationsvorgang wird der Router neu gestartet, danach ist das neue Web-Interface unter der Adresse **http://192.168.1.1:8080/** erreichbar. Falls Sie eine Fehlermeldung erhalten, dass keine Verbindung hergestellt werden konnte, so warten Sie bitte einen Moment und laden die Seite dann neu.

5. Die Zugangsdaten für das Web-Interface sind:

   Benutzer: **root**
   Passwort: **admin**

1.2 Netgear WNDR3700

Der Router kann über das Web-Interface der Original-Firmware mit der Firmware von HOTSPLOTS geflasht werden:

1. Starten Sie einen Webbrowser und verbinden Sie ihn mit dem Router, so wie in dessen Bedienungsanleitung beschrieben. Es ist nicht erforderlich, Software von der mitgelieferten CD zu installieren, auch wenn dies als Hinweis vermerkt ist.

In Werkseinstellung lässt sich das Webinterface der Originalfirmware unter http://192.168.1.1 aufrufen.
Nutzername: admin
Passwort: password

2. Wählen Sie dann den Menüpunkt ***„Wartung – Router aktualisieren - Firmware Upgrade“.***

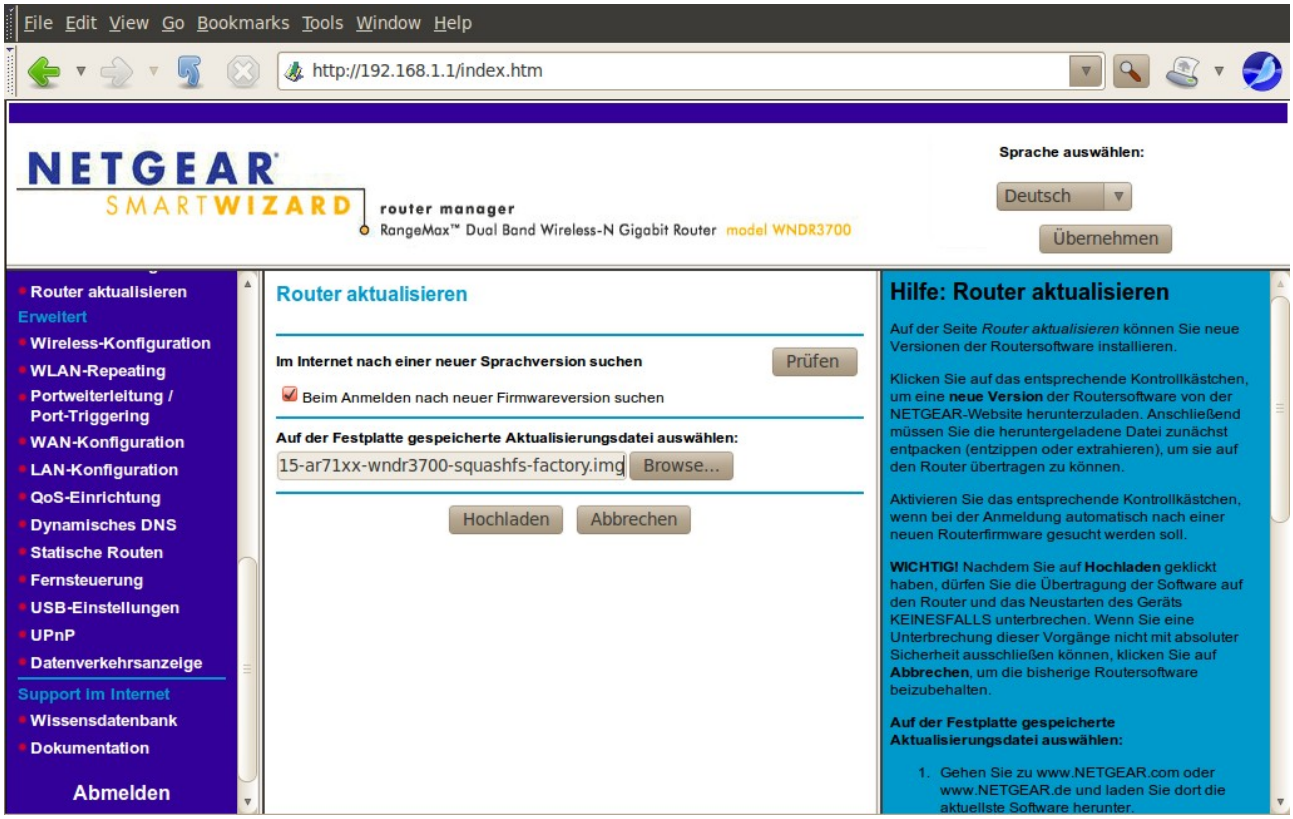


Abbildung 2: Das Webinterface der Originalfirmware von Netgear zum Upgrade auf die Firmware von HOTSPLOTS

3. Wählen Sie als Datei ein Firmware-Image von HOTSPLOTS aus:
hotsplotsWrt-3.0-___-ar71xx-tl-wndr3700-v_-squashfs-factory.bin[1]
Achten Sie dabei auf den Namensteil „factory“!

4. Führen sie nun das Upgrade aus. Nach dem Installationsvorgang wird der Router neu gestartet, danach ist das neue Web-Interface unter der Adresse **http://192.168.1.1:8080/** erreichbar. Falls Sie eine Fehlermeldung erhalten, dass keine Verbindung hergestellt werden konnte, so warten Sie bitte einen Moment und laden die Seite dann neu.

5. Die Zugangsdaten für das Web-Interface sind:

   Benutzer: root
   Passwort: admin

1 Die Unterstriche sind Platzhalter für die genaue Version der Firmware bzw. die Hardwareversion Ihres Router.

2 Anschließen des Hotspot-Routers

Mit Hotspot-Router wird der WLAN-Router bezeichnet, auf dem das Hotspot-Portal (chilli), die eigentliche Hotspot-Funktion, läuft. Dieser Router verteilt die IP-Adressen an die Funk-Clients sowie bei aktivierter Netzwerkbrücke auch an die per LAN verbundenen Clients und überwacht den Zugriff auf das Internet.

Zurzeit gibt es keinen Router mit integriertem DSL-Modem, auf dem eine passende Firmware stabil läuft (Stand Dezember 2011). Für die Verbindung zum Internet ist daher entweder ein weiterer Router (mit Uplink ins Internet) oder ein DSL-Modem nötig.

2.1 Anschluss des Admin-PCs zur Konfiguration

Stellen Sie die Netzwerkverbindung Ihres PCs auf die IP-Adresse 192.168.1.2, Subnetzmaske 255.255.255.0 ein und verbinden Sie die so konfigurierte Netzwerkkarte per Netzwerkkabel mit einem der LAN-Ports „1-4“ des Routers.

Die Administrationsoberfläche erreichen Sie mit Ihrem Webbrowser über die URL **http://192.168.1.1:8080/**. Anschließend werden Sie nach Nutzernamen und Passwort gefragt. Der Standardwert für den Nutzernamen ist **root** und für das Passwort **admin**.

Dann sollten Sie die Startseite der Administrationsoberfläche sehen.

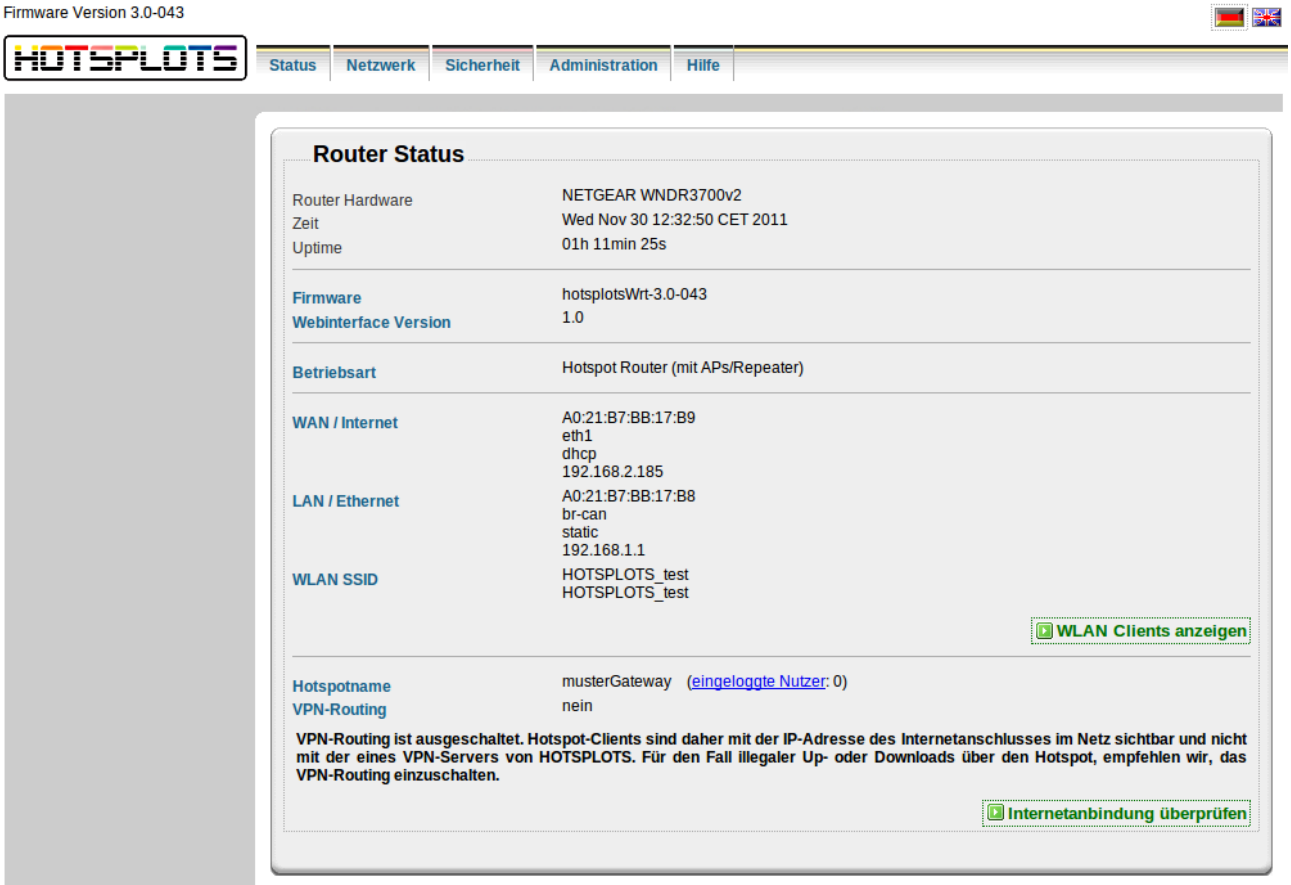


Abbildung 3: Status-Seite des Webinterfaces

2.2 Anschluss an DSL-Modem

Zum Internet erfolgt der Anschluss des Hotspot-Routers über den WAN-Port, der sich auf der Rückseite des Routers befindet (TP-LINK: blaue Buchse, Netgear: gelbe Buchse)

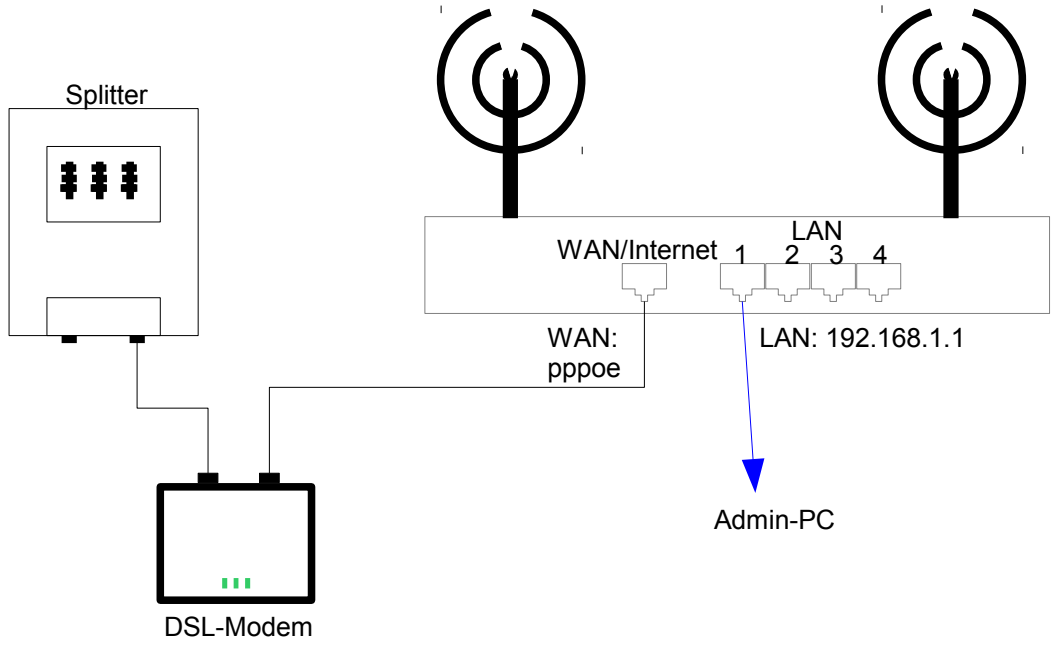


Abbildung 4: Anschluss an DSL-Modem

Abbildung 5: Eingabe der DSL-Zugangsdaten

Wenn der Router per Netzwerkkabel an ein DSL-Modem angeschlossen wird, müssen auf dem Hotspot-Router die DSL-Zugangsdaten hinterlegt werden. Gehen Sie dafür auf den Menüpunkt ***Netzwerk >> WAN / Internetanbindung*** (siehe Abb. 5). Wählen Sie dort ***„PPPoE (über DSL-Modem)“*** aus. Die Seite wird dann neu aufgebaut und Eingabefelder für DSL-Nutzername und DSL-Passwort erscheinen.

Tragen Sie dort die Daten ein, die Sie von Ihrem DSL-Provider bekommen haben. Falls Ihr Anbieter Ihnen zwar einen Nutzernamen (z. B. Ihre Telefonnummer) aber kein Passwort mitgeteilt hat, kann es sein, dass die Einwahl nicht funktioniert, wenn Sie das Feld leer lassen; tragen Sie in dem Fall irgendetwas ein.

In der Werkseinstellung ist als Verbindungsart *„permanent“* ausgewählt. Dies ist zu empfehlen, da der Router so eine kontinuierliche Verbindung zum Internet und zu unseren VPN-Servern aufrecht erhalten kann. Sollten Sie eine Internetanbindung haben, die zeitbasiert abgerechnet wird, achten Sie bitte darauf, dass Ihnen durch die permanente Anbindung Kosten entstehen können.

2.3 Anschluss hinter (DSL-)Router

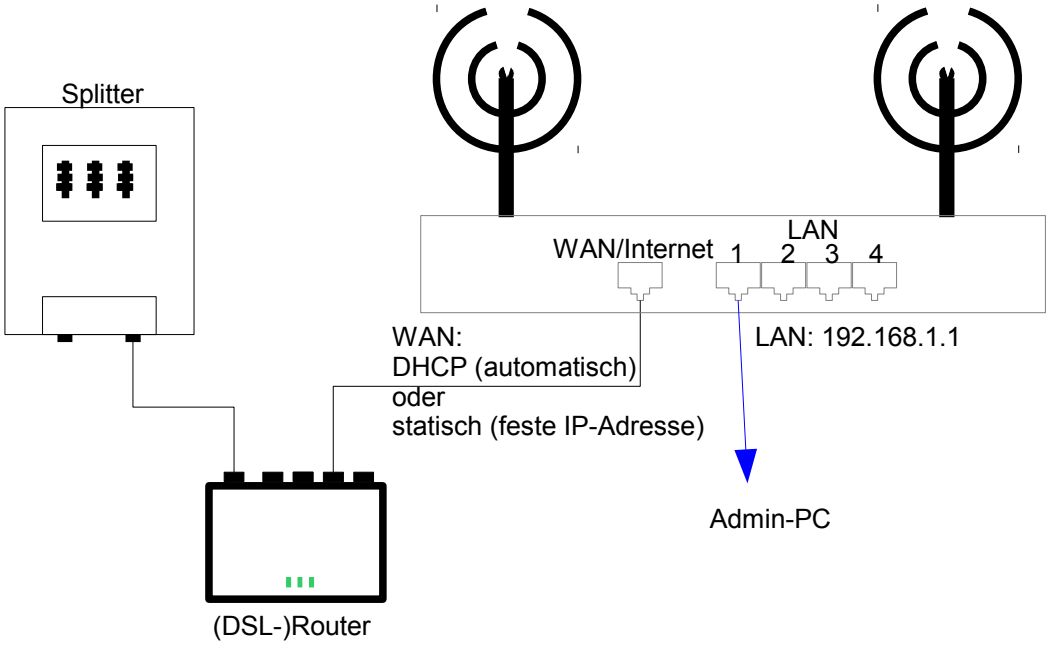


Abbildung 6: Anschluss an (DSL-)Router

Zum Internet erfolgt der Anschluss des Hotspot-Routers über den WAN-Port, der sich auf der Rückseite des Routers befindet (TP-LINK: blaue Buchse, Netgear: gelbe Buchse).

Wenn der Hotspot-Router in ein bestehendes LAN integriert oder an einen Internet-Router angeschlossen werden soll, so verbinden Sie die den WAN-Port des Hotspot-Routers mit einem LAN-Port Ihres Internet-Routers bzw. mit einem damit verbundenen Switch, siehe Abbildung 6.

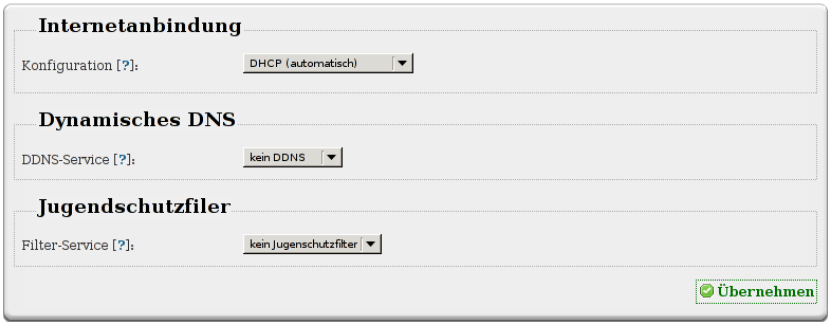


Abbildung 7: Standardeinstellung für den WAN-Port: DHCP (automatisch)

Wenn Ihr Internet-Router per DHCP automatisch IP-Adressen zuweist, dann können Sie die Standardeinstellung für Internet (WAN) *„DHCP (automatisch)“* stehen lassen und müssen nichts weiteres eintragen, siehe Abb. 7.

Dabei ist jedoch darauf zu achten, dass die per DHCP bezogene IP-Adresse des WAN-Ports in einem anderen Subnetz liegen muss als die IP-Adresse des LAN-Ports. Sonst funktioniert das Routing nicht, der Router kommt nicht ins Internet und kann auch keine IP-Adressen an WLAN-Clients verteilen. Sollte dieser Fehler auftreten, kann er leicht durch Ändern der LAN-IP-Adresse beseitigt werden, etwa durch Ersetzen von 192.168.1.1 durch 192.168.43.1.

2.4 Überprüfen der Internet-Verbindung

Die Internetverbindung kann auf der Status-Seite mit dem Button „Internetverbindung prüfen“ geprüft werden. Es wird nur die Internetverbindung über den WAN-Port geprüft. Bei Repeatern, die per WLAN angebunden sind oder kabelgebundenen Access Points funktioniert die Prüfung über das Webinterface nicht.

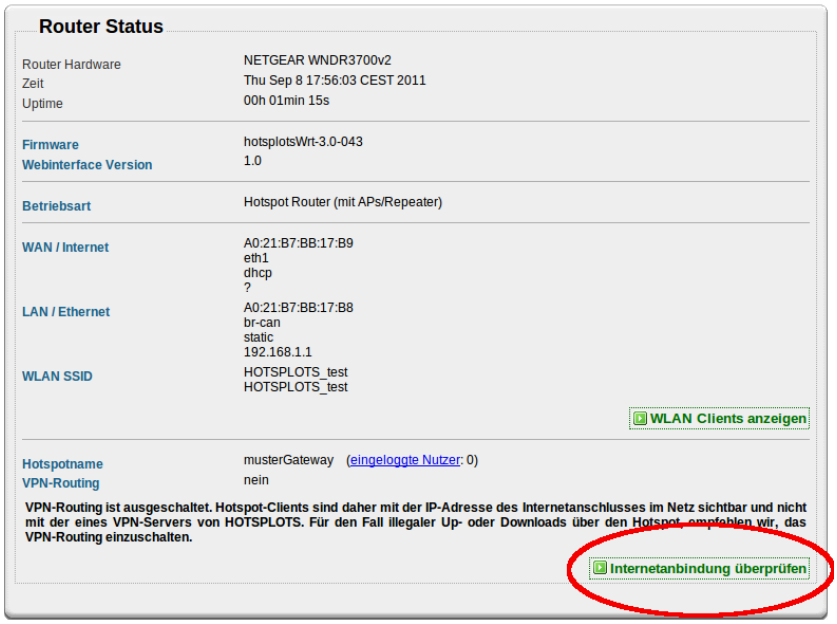


Abbildung 8: Kontaktierung eines HOTSPLOTS Servers zum Überprüfen von Internetzugang und Einstellungen

3 Erweiterung mit Repeatern oder Access Points

Es ist möglich, das vorhandene Netzwerk durch Hinzunahme weiterer Router zu erweitern:

1. Empfehlenswert ist der Anschluss sog. Access Points (APs) per Netzwerkkabel an den LAN-Ports des Hotspot-Routers.
2. Die Funkbereiche von WLAN-Router und Access Points können durch Einsatz weiterer Sender im Repeater-Modus vergrößrt werden.

WICHTIG: Wenn das Netzwerk um zusätzliche Accesspoints oder Repeater erweitert werden soll, stellen Sie bitte unter dem Menüpunkt ***Netzwerk*** den Betriebsmodus des Hotspot-Routers auf den Wert „***Hotspot Router (mit APs/Repeater)***“. Hierdurch werden das WLAN-Interface und das LAN-Interface miteinander gebrückt. Um an den Hotspot-Router weitere APs oder Repeater anzuschließen, ist dieser Betriebsmodus erforderlich. Des Weiteren empfehlen wir, allen Access Points und Repeatern im Netzwerk eine LAN-IP im selben Subnetz zu geben, um diese später über das Netzwerk administrieren zu können.
Alle notwendigen Einstellungen können auf der Administrationsoberfläche der HOTSPLOTS Firmware vorgenommen werden.

3.1 Konfiguration als Access-Point zum Anschluss per Netzwerkkabel

Grundsätzlich kann jeder standardkonforme Access Point an den Hotspot-Router angeschlossen werden. Wichtig ist, dass es sich wirklich um einen Access Point, also eine transparente Brücke (Bridge) zwischen WLAN und LAN handelt und nicht um einen Router, der selbst die Funktion der NAT (Network Address Translation) übernimmt. Anleitung und Support können wir nur für Geräte mit der HOTSPLOTS eigenen Firmware leisten. Außerdem ist nur bei Geräten mit HOTSPLOTS Firmware sichergestellt, dass die netzweite Client-Isolierung ordnungsgemäß funktioniert (siehe S. 21).

Um den Router als Access Point zu betreiben, muss der Betriebsmodus umgestellt werden. Dazu wird auf der Netzwerk-Status-Seite (Netzwerk) der Betriebsmodus „Access Point“ gewählt. Nach dem automatischen Neustartet arbeitet der Router als Access Point.

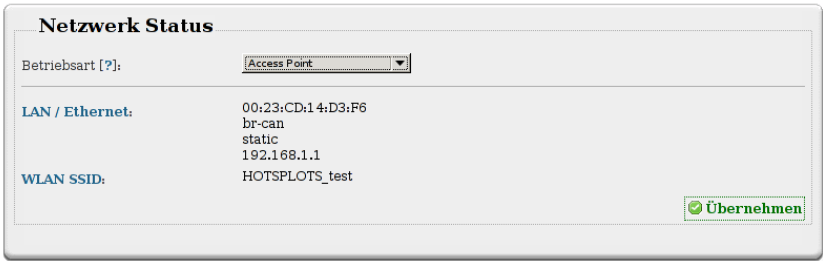


Abbildung 9: Einstellung für kabelgebundene Access Points

WICHTIGER HINWEIS: Die Verbindung zum Router per Netzwerkkabel muss wie in Abbildung 10 skizziert über einen der **LAN-Ports** erfolgen! Der WAN-Port ist in dieser Konfiguration nicht von Bedeutung.Wichtig ist nur, dass ihm keine IP-Adresse aus dem Subnetz der LAN-Ports zugewiesen wird.

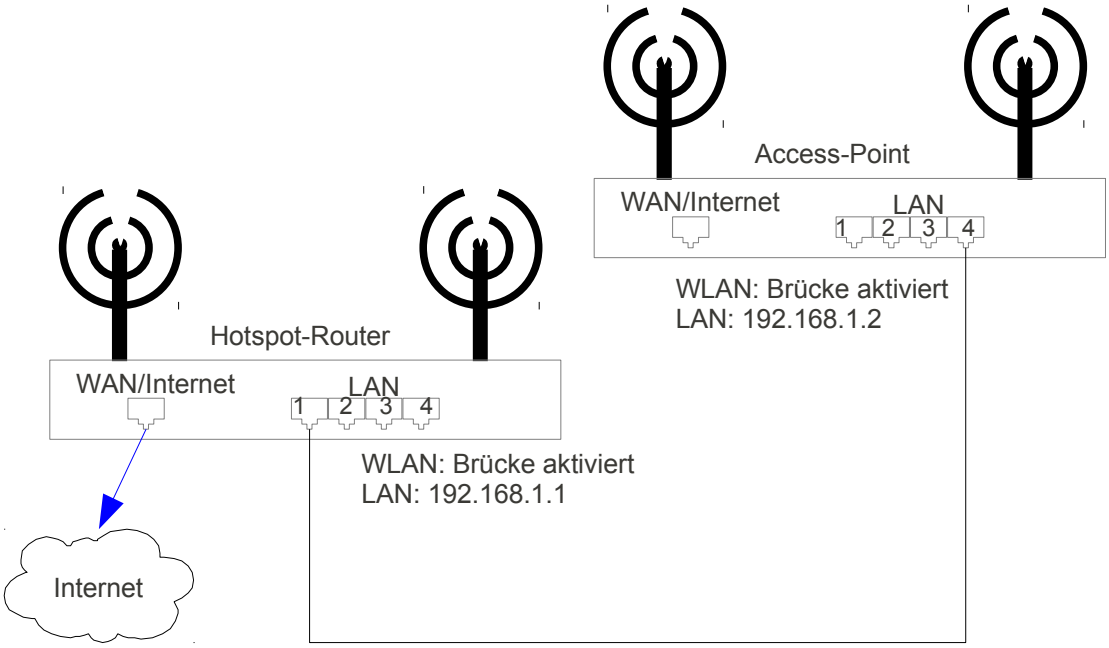


Abbildung 10: Anschluss an (DSL-)Router

TIPP: Wenn Sie für den Access-Point dieselbe SSID eintragen wie für den Hotspot-Router, dann können Sie sich ohne Verbindungsabbruch mit dem Notebook vom Empfangsbereich des einen in den des anderen bewegen.

TIPP: Zu Wartungszwecken ist es hilfreich, die LAN-Adresse statisch zu konfigurieren. Dann können Sie sich vom Hotspot-Router per ssh darauf einloggen. Eine Fernwartung ist möglich, indem man sich per ssh zuerst auf dem Hotspot-Router einloggt und von dort aus auf den weiteren APs bzw. Repeatern.

Achtung: Beim Aktivieren des Betriebsmodus „Access Point“ wird automatisch der DHCP-Server unter LAN deaktiviert. Dieser darf nicht manuell wieder angeschaltet werden!

3.2 Konfiguration als WLAN-Repeater

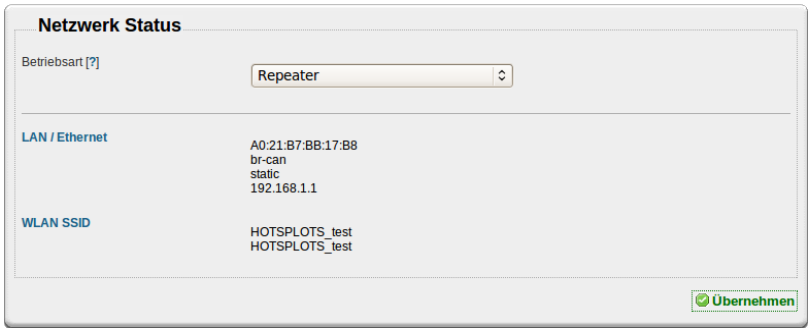


Abbildung 11: Auswahl der Betriebsart "Repeater"

Repeater reduzieren die effektive Bandbreite in WLANs! Um den Router als Repeater zu betreiben, muss der Betriebsmodus umgestellt werden. Dazu wird auf der Netzwerk-Status-Seite (Netzwerk) der Betriebsmodus *„Repeater“* gewählt. Bitte beachten Sie, dass sich Hotspot-Router als auch der Repeater im selben WLAN-Netzwerk befinden müssen. Nach dem automatischen Neustart arbeitet der Router als Repeater.

Um den Repeater auf das Funknetz einzustellen, wählen Sie die Seite *„Netzwerk >> WLAN / Funknetz“*. Tragen Sie dort im oberen Feld „Funkeinstellungen Repeater“ die Einstellungen für das Funknetz ein, dass der Repeater erweitern soll. Wir empfehlen, lediglich im Feld *„MAC-Adresse der Gegenstelle“* die physikalische WLAN-Adresse des Gerätes einzutragen, auf welches der Repeater eine Verbindung herstellen soll. Das Feld *„SSID der Gegenstelle“* ist optional und sollte leer sein, wenn Sie das Feld *„MAC-Adresse der Gegenstelle“* gefüllt haben. Lassen Sie wiederum das Feld *„MAC-Adresse der Gegenstelle“* leer, verbindet sich das Gerät automatisch mit dem Gerät im Netzwerk, dessen SSID im unteren Feld *„SSID der Gegenstelle“* eingetragen ist. Achten Sie hierbei auf Eindeutigkeit der SSID, um zu verhindern, dass Repeater sich gegenseitig verbinden, ohne eine Verbindung zu einem AP oder Router zu haben.

Achten Sie bitte auch darauf, dass der Kanal identisch mit den Funkeinstellungen des Hotspot-Routers ist. Andernfalls kann das Funknetz nicht erweitert werden.

Besonderheit bei Netgear WNDR3700: *Da dieses Gerät sowohl das 2,4 GHz als auch das 5 GHz-Band unterstützt, können Sie in der Firmware dieses Gerätes wählen, für welchen Frequenzbereich die Einstellungen gelten sollen.*

Im zweiten Feld „HOTSPLOTS WLAN“ können Sie die SSID des Repeaters selbst einstellen. Mit dieser SSID können sich Hotspot-Gäste mit dem Hotspot verbinden. Ein Screenshot für diese Einstellungen sehen Sie in Abbildung 12.

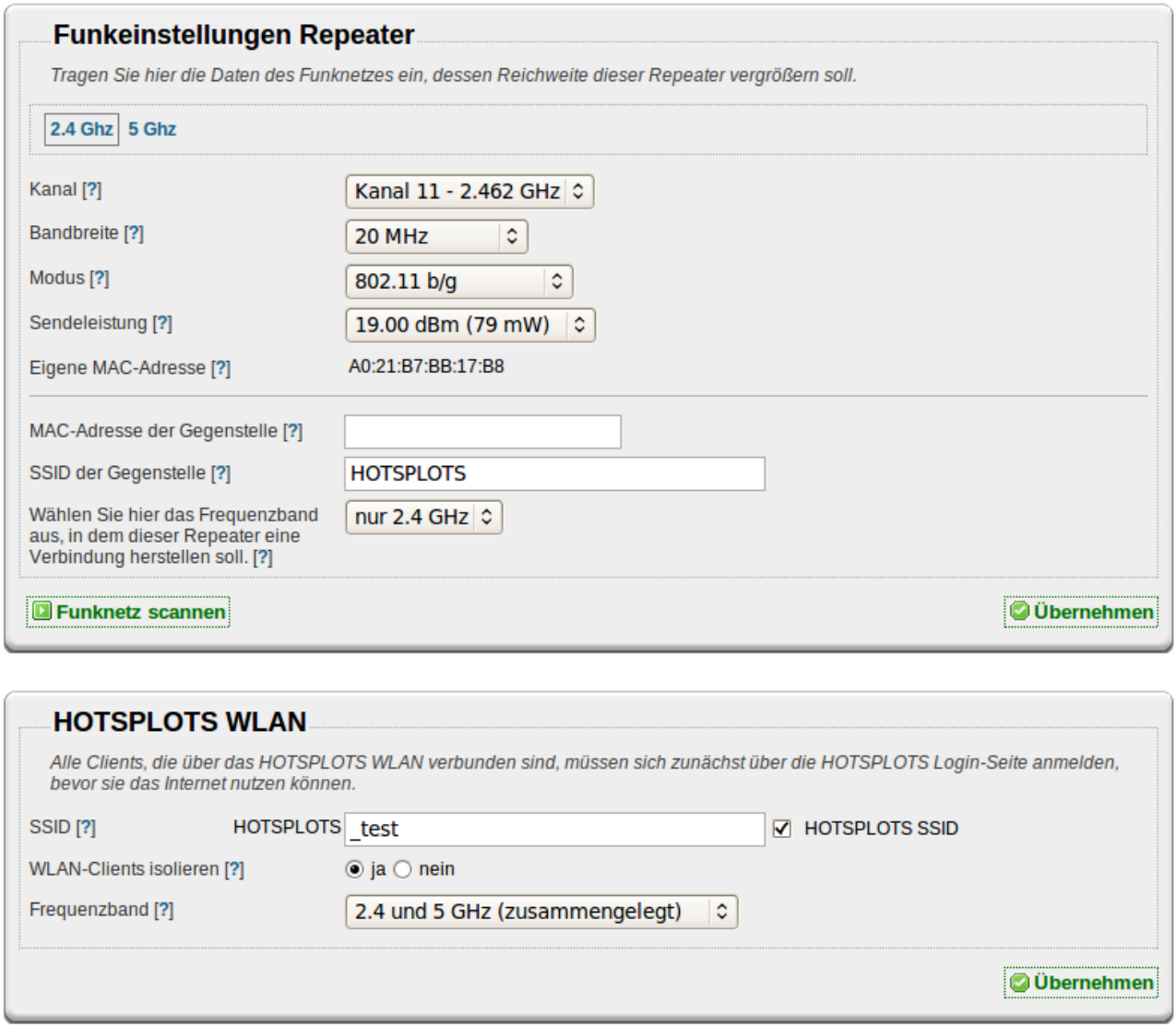


Abbildung 12: Konfiguration eines Repeaters

Achtung: Beim Aktivieren der Betriebsart „Repeater“ wird automatisch der DHCP-Server unter LAN deaktiviert. Dieser darf nicht manuell wieder angeschaltet werden!

Zu Wartungszwecken ist es hilfreich, die LAN-Adresse statisch zu konfigurieren. Bei Fernwartung können Sie sich vom Hotspot-Router per SSH darauf einloggen oder bei entsprechend gesetzter Port-Weiterleitung auch auf das Web-Interface zugreifen.

4 Die Firmware-Menüpunkte im Überblick

4.1 Die Status-Seite

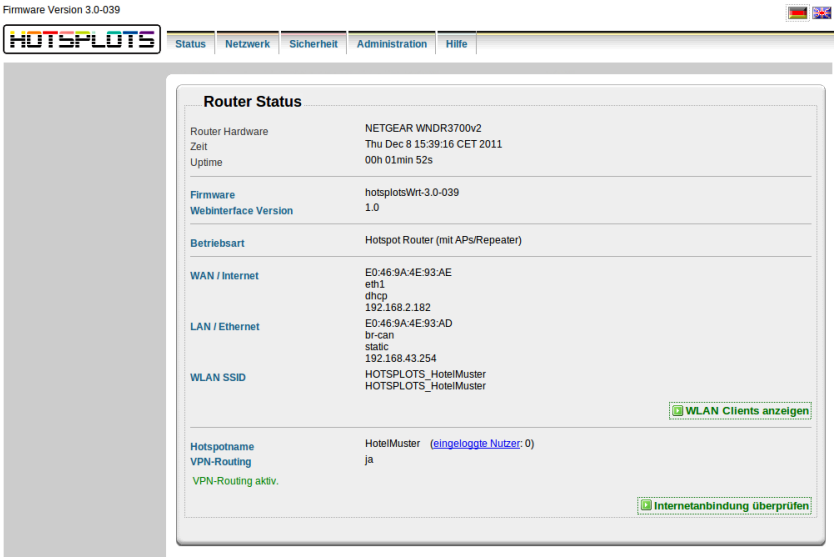


Abbildung 13: Status-Seite

Die Status-Seite gibt eine Übersicht über die verwendete Hardware, die Version der Firmware und eben den Status.

Um zu den einzelnen Menüpunkten zu gelangen, reicht es aus, auf den jeweiligen Bezeichner zu klicken.

Die Zeit holt sich das Gerät bei jedem Neustart von einem NTP-Server im Internet. Für die Basisfunktion des Hotspots ist eine korrekte Zeit nicht zwingend notwendig, allerdings für die Nutzung des optionalen VPN-Routings.

Von den Netzwerkkarten für WAN und LAN werden IP-Adressen und MAC-Adresse angezeigt.

Wenn VPN-Routing aktiv ist, werden alle Verbindungen der Hotspot-Nutzer nicht direkt in das Internet geroutet sondern über einen Server von HOTSPLOTS.

„Hotspot-Name“ gibt den eindeutigen Namen des Hotspots an, so wie er zuvor im Kundenbereich generiert wurde.

4.2 Netzwerk

Abbildung 14: Menüpunkte Netzwerk

WAN / Internetanbindung

Auf der Seite *WAN / Internetanbindung* werden die Einstellungen für die Netzwerkbuchse zum WAN (Wide Area Network, typischerweise das Internet) vorgenommen. Diese Einstellungen müssen Sie nur am ersten Gerät, dem Hotspot-Router, vornehmen.

Bei Repeatern oder einfachen APs müssen auf dieser Seite keine Einstellungen vorgenommen werden.

Internetanbindung

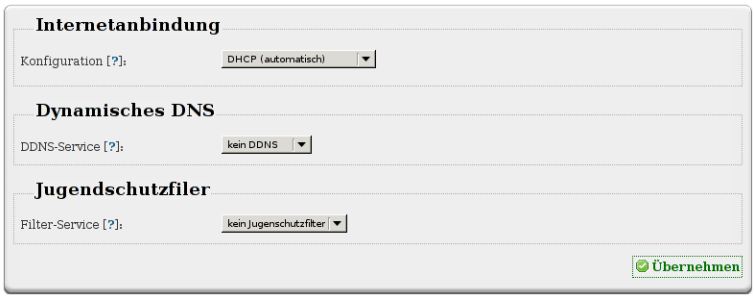


Abbildung 15: WAN / Internetanbindung

Im obersten Pulldown-Menü, *Internet (WAN)*, gibt es 4 Betriebsmodi:

1. *PPPoE (DSL-Modem)* ist richtig, wenn der Router direkt an ein DSL-Modem angeschlossen ist. Bei Auswahl dieser Betriebsart am WAN-Port lädt die Seite neu und Felder für die Eingabe der PPPoE-Einwahldaten werden angezeigt. Tragen Sie hier die Zugangsdaten ein, die Sie von Ihrem ISP *(Internet Service Provider, Ihrem Internetanbieter)* bekommen haben. Manche ISPs verlangen an dieser Stelle nur einen Nutzernamen. Tragen Sie in diesem Fall in das Feld *Passwort* einen beliebigen Wert ein.
2. *DHCP (automatisch)* ist richtig, wenn der Hotspot-Router an einen (DSL-)Router angeschlossen wird, der per DHCP-Server automatisch IP-Adressen vergibt. Näheres in Kap. 2.3.
3. *Statisch (feste IP-Adresse)* ist richtig, wenn der Hotspot-Router an einen (DSL-)Router angeschlossen wird, dessen LAN Sie manuell konfigurieren. Näheres ebenfalls in Kap. 2.3.
4. *nicht genutzt (aus)* ist nur sinnvoll für Repeater oder kabelgebundene Access Points. Hotspot-Router, die den Zugang zum Hotspot und damit zum Internet regeln sollen, können mit dieser Einstellung nicht funktionieren.

Dynamisches DNS

Dynamisches DNS brauchen Sie nur, wenn es sich um einen direkt ans Internet - also in aller Regel per PPPoE an ein DSL-Modem angeschlossenen - Hotspot-Router handelt und dieser aus dem Internet erreichbar

sein soll. Das kann etwa zur Fernwartung nützlich sein oder wenn Sie lokal Serverdienste betreiben. Portweiterleitungen zu diesen Serverdiensten können Sie unter ***Sicherheit >> Firewall*** einrichten.
Als Anbieter für den Service sind dyndns.org, easydns oder zoneedit vorgesehen.

Die IP-Adresse des Internetanschlusses wird übrigens im Kundenbereich unter dem Menüpunkt Meine Hotspots angezeigt. Damit kann man auch ohne DynDNS Standorte mit dynamischer IP-Adresse fernwarten.

Jugendschutzfilter

Für spezielle Standorte wie Schulen und Kinderbibliotheken bieten wir eine Schnittstelle zu dem externen Dienst von OpenDNS.

Näheres siehe http://www.hotsplots.de/fileadmin/media/flyers/HOTSPLOTS_Jugendschutz.pdf.

Welche Webseiten gesperrt werden sollen, kann über das (englische) Webinterface von OpenDNS gesteuert werden. Nach Registrierung unter http://www.opendns.com können Sie hier Ihren OpenDNS-Nutzernamen und das OpenDNS-Passwort sowie den Netzwerknamen eintragen.

Bitte haben Sie Verständnis dafür, dass wir für diesen Dienst keinen Support leisten können.

LAN / lokales Ethernet

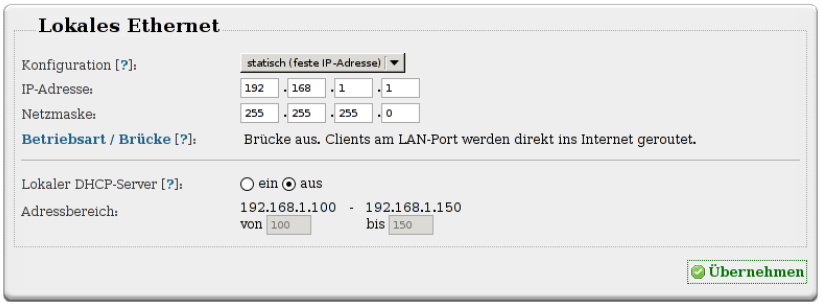


Abbildung 16: LAN Einstellungen

Für ***LAN / lokales Ethernet*** ist die statische Konfiguration voreingestellt. Die LAN-Ports können auch deaktiviert werden, was in der Regel aber nicht sinnvoll sein dürfte. Typischerweise werden Sie mit der Netzmaske 255.255.255.0 gut bedient sein. Damit können 254 PCs verwaltet werden.

Die Standardeinstellung für die IP-Adresse ist **192.168.1.1.** Wenn der Hotspot-Router in ein bereits vorhandenes LAN integriert werden soll, das auch Adressen im Bereich 192.168.1.xxx benutzt und der WAN-Anschluss in diesem Bereich liegen soll, dann können Sie hier eine andere IP-Adresse wie etwa 192.168.43.xxx auswählen. Alles mit 192.168.44.xxx ist tabu, denn in dem Bereich werden IP-Adressen an die Hotspot-Clients verteilt.

Der DHCP-Server hat nichts mit dem Verteilen von IP-Adressen an WLAN-Clients zu tun, sondern betrifft nur Rechner, die per Kabel mit dem LAN-Port verbunden sind und auch das nur dann, wenn die Betriebsart „Hotspot Router (ohne APs)“ ist. Es betrifft also nur Rechner, die über den integrierten Switch an das Internet angeschlossen werden sollen und sich nicht am Hotspot authentifizieren müssen.
Wenn der DHCP-Server aktiv ist, können Sie mit einem PC, der die IP-Adresse automatisch bezieht (so, wie es bei Windows voreingestellt ist) das Webinterface aufrufen ohne die Netzwerkkarte konfigurieren zu müssen.

WLAN / Funknetz

Auf der Seite ***WLAN / Funknetz*** können allgemeine Funkeinstellungen festgelegt werden.
Den **Kanal** sollten Sie so wählen, dass möglichst wenig weitere Sender auf demselben Kanal oder den unmittelbaren Nachbarkanälen stören können. Welche anderen WLAN-Sender aktiv sind, können Sie näherungsweise mit Ihrem Betriebssystem und Treibersoftware sehen. Sehr empfehlenswert für Windows-Rechner sind die kostenlosen Tools InSSIDer, vistumbler oder netstumbler.
Sie können zwischen den Kanälen 1 bis 13 wählen. Die Kanäle 12 und 13 gehören jedoch nicht zum amerikanischen Standard. Um niemanden auszugrenzen, empfehlen wir daher dringend, öffentliche Hotspots auf die Kanäle 1 bis 11 zu beschränken. Des Weiteren ist, sofern möglich, die Wahl sog. überlappungsfreier

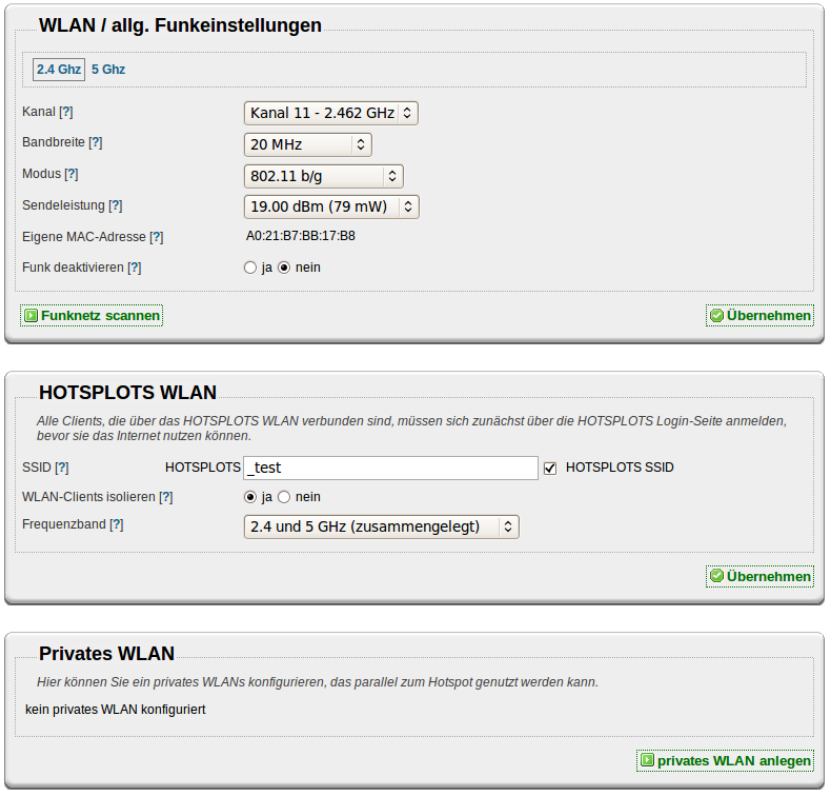


Abbildung 17: WLAN Einstellungen

Kanäle (Kanäle 1, 6 und 11) ratsam, sofern die angeschlossenen Geräte als Accesspoint konfiguriert sind. Mit dem Router verbundene Repeater müssen auf den gleichen Kanal wie dem des Routers eingestellt werden.

Die **Bandbreite** steuert die Übertragungsrate des WLAN-Netzes. Bei einer Bandbreite von 40MHz kann eine höhere Übertragungsgeschwindigkeit erreicht werden, wenn die Funkumgebung des Hotspots dies zulässt. Da die Übertragung bei 40MHz empfindlicher gegenüber Störungen ist, empfehlen wir diesen Wert auf 20 MHz belassen.

Der **Modus** legt fest, in welchem Funkstandard das Gerät operieren soll. Die Standardeinsellung ist noch 802.11 b/g, welche eine maximale Datenübertragungsrate von 54 Mbit/s gewährleistet. Mit dem Modus 802.11n kann man einehöhere Datenübertragungsrate und vor allem bei der Verwendung in Gebäuden eine höhere Reichweite erreichen. Einige wenige WLAN-Clients (Endgeräte) weisen zum aktuellen Zeitpunkt (Stand Oktober 2011) noch Stabilitätsprobleme auf. Sollten demnach bei Verwendung des Modus 802.11n Funktionsprobleme oder Fehler auftreten, raten wir, zum Standard 802.11 b/g zu wechseln.

Die **Sendeleistung** kann zwischen 10 und 100 mW eingestellt werden. Dabei gilt, dass mehr nicht unbedingt besser ist, denn mit steigender Leistung nimmt auch das Rauschen zu und es bringt nichts, wenn der Sender zwar sehr stark sendet, die Gegenstellen aber nicht ebenso stark zurücksenden können. Außerdem ist in Deutschland die maximal erlaubte Sendeleistung auf 100 mW (entspricht 20 dBm) effektive Sendeleistung (EIRP) beschränkt. Da die mitgelieferten Antennen typischerweise eine Verstärkung von 2 dBi aufweisen, sind nur noch 18 dBm in Deutschland erlaubt. Bei Bedarf kann der Funk über die Option **Funk deaktivieren** ganz ausgeschaltet werden. Dies ist nur in speziellen Fällen sinnvoll, in denen die Hotspot-Funktionalität nur an den LAN-Anschlüssen gewünscht wird.

Die **SSID** ist der Name des Drahtlosnetzwerkes, den Nutzer auswählen müssen, bevor sie die Login-Seite sehen können. Die SSID beginnt sollte immer mit „HOTSPLOTS“ beginnen. Am besten tragen Sie dahinter den Namen ein, den Sie beim Anlegen des Hotspots im Kundenbereich der Website angegeben haben. Dann ist den Nutzern die Verbindung zwischen Daten auf der Hotspot-Karte, ggf. auf Location Tickets und der SSID ersichtlich. In Ausnahmefällen kann die Standardoption HOTSPLOTS SSID ausgeschaltet werden. Das ist vor allem für Hotspots mit dem Tarif V.I.P. /Nur Tickets gedacht.

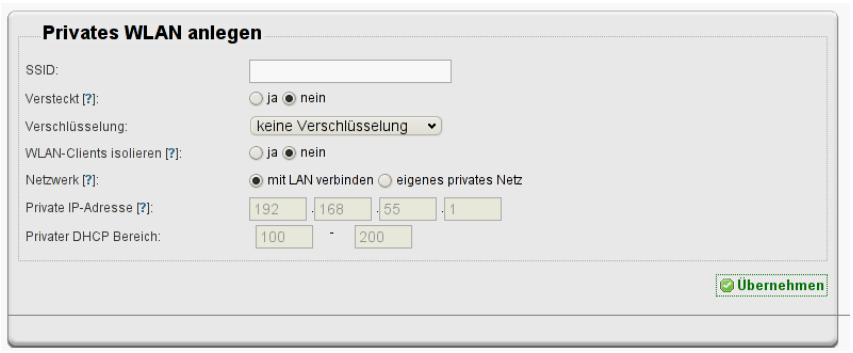


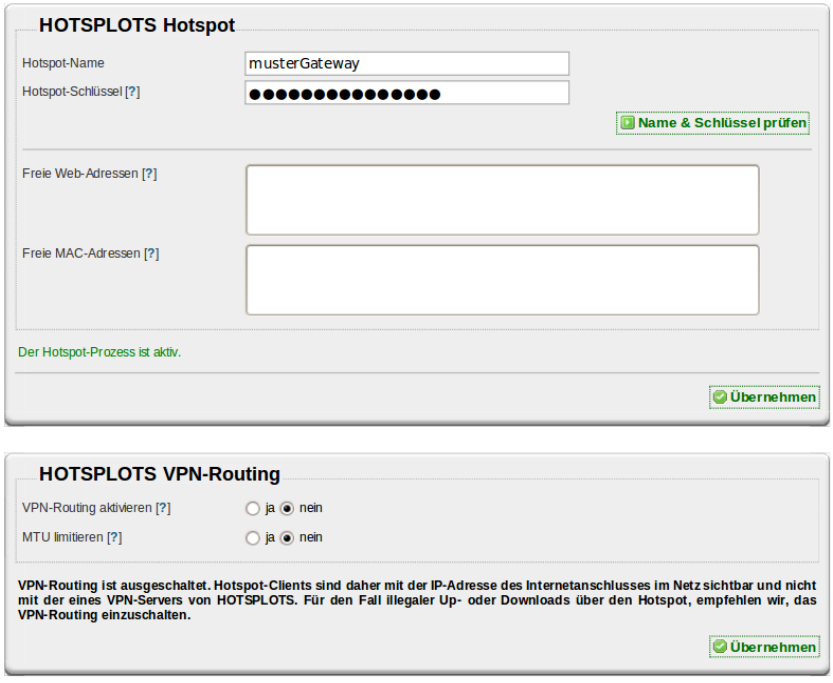
Abbildung 18: Neues Netzwerk anlegen

Des Weiteren besteht die Möglichkeit, ein **privates Funknetz** anzulegen. Clients, die sich in diesem Funknetz einbuchen, werden wie lokale LAN-Clients des Routers behandelt und werden direkt ohne Anmeldung und VPN-Routing ins Internet geroutet.

Alternativ kann für das private WLAN ein **eigenes privates Netz** mit einer eigenen IP-Adresse angelegt werden. In diesem Fall bekommen WLAN-Clients im privaten Netz per DHCP eine IP-Adresse im ausgewählten Bereich zugewiesen und werden analog wie lokale Clients ohne Anmeldung und VPN-Routing behandelt. Mit der Option **Versteckt** können Sie die SSID des privates WLANs unsichtbar machen. Unter **Verschlüsselung** können Sie eine Verschlüsselung für Ihr privates WLAN auswählen. Beachten Sie bitte, dass die Länge des WPA2-Keys zur Verschlüsselung mindestens 8 Zeichen betragen muss!

Achtung: Ein verstecktes Funknetzwerk, das nicht durch eine Verschlüsselung geschützt ist, bietet keinen Schutz. Es ist für andere Personen weiterhin möglich eine Verbindung aufzubauen, auch wenn der Name nicht sichtbar ist.

HOTSPLOTS Hotspot



Die Felder ***Hotspot-Name*** und ***Hotspot-Schlüssel*** sind genau mit den Daten auszufüllen, die Sie im Kundenbereich auf www.hotsplots.de beim Anlegen des Hotspots angegeben haben. Anhand dieser Daten authentifiziert sich der Hotspot gegenüber dem HOTSPLOTS-Server. Diese Authentifizierung kann mit dem Button *„Gateway & Schlüssel prüfen“* getestet werden. Damit wird gleichzeitig die Internetverbindung überprüft.

Abbildung 19: HOTSPLOTS spezifische Einstellungen

In das Feld ***Freie Web-Adressen*** können Seiten eingegeben werden, die ohne Authentifizierung erreichbar sein sollen. Diese Funktion von Hotspots wird häufig als Walled Garden bezeichnet. Die Sites www.hotsplots.de, shop.hotsplots.de und www.paypal.de sind immer freigeschaltet. Die maximal mögliche Anzahl an Sites ist nicht begrenzt.

Mit dem Feld ***Freie MAC-Adressen*** können Netzwerkkarten freigeschaltet werden, so dass deren Nutzer sich nicht mehr authentifizieren müssen. Wenn es sich dabei um WLAN-Karten handelt, beinhaltet diese Option ein gewisses Risiko: Jeder Nutzer, der sich ein wenig auskennt, kann die MAC-Adressen weiterer laufender Funkverbindungen mitlesen (sniffen), anschließend seiner eigenen Netzwerkkarte eine dieser

MAC-Adressen zuweisen und sich so gegebenenfalls unberechtigten Zugang zum Internet verschaffen. Eingeführt wurde diese Option als Notlösung für mobile Geräte ohne Webbrowser, wie etwa eine Playstation Portable, aber auch in Hotels mit kabelgebundenen (Bezahl-)Terminals wird es gern für ebenfalls kabelgebundene Rechner an der Rezeption verwendet.

HOTSPLOTS VPN-Routing

Wenn die Option ***VPN-Routing*** aktiviert ist, wird der gesamte Traffic des Hotspots über einen Server von HOTSPLOTS geroutet. Diese Option ist eine Schutzfunktion für Hotspot-Betreiber. Wenn das VPN-Routing aktiviert ist, ist aus dem Internet nicht die IP-Adresse des Hotspots zu sehen sondern die Adresse eines Servers von HOTSPLOTS.

Die Nutzung dieses Service ist kostenfrei.

Zwar erhöhen sich dadurch zwangsläufig die Pingzeiten und man hat eine zusätzliche Fehlerquelle, die unter Umständen zu (wahrscheinlich kurzen) Ausfallzeiten führen kann, die Verwendung von VPN-Routing wird aber dennoch ausdrücklich empfohlen.
Sollte ein VPN-Server ausfallen, wird automatisch eine Verbindung zu einem anderen VPN-Server aufgebaut.

Verbindungen von Nutzern, die selbst die optionale Verschlüsselung mit OpenVPN nutzen, werden immer über einen Server von HOTSPLOTS geroutet – unabhängig von der Einstellung auf dieser Seite.

4.3 Sicherheit

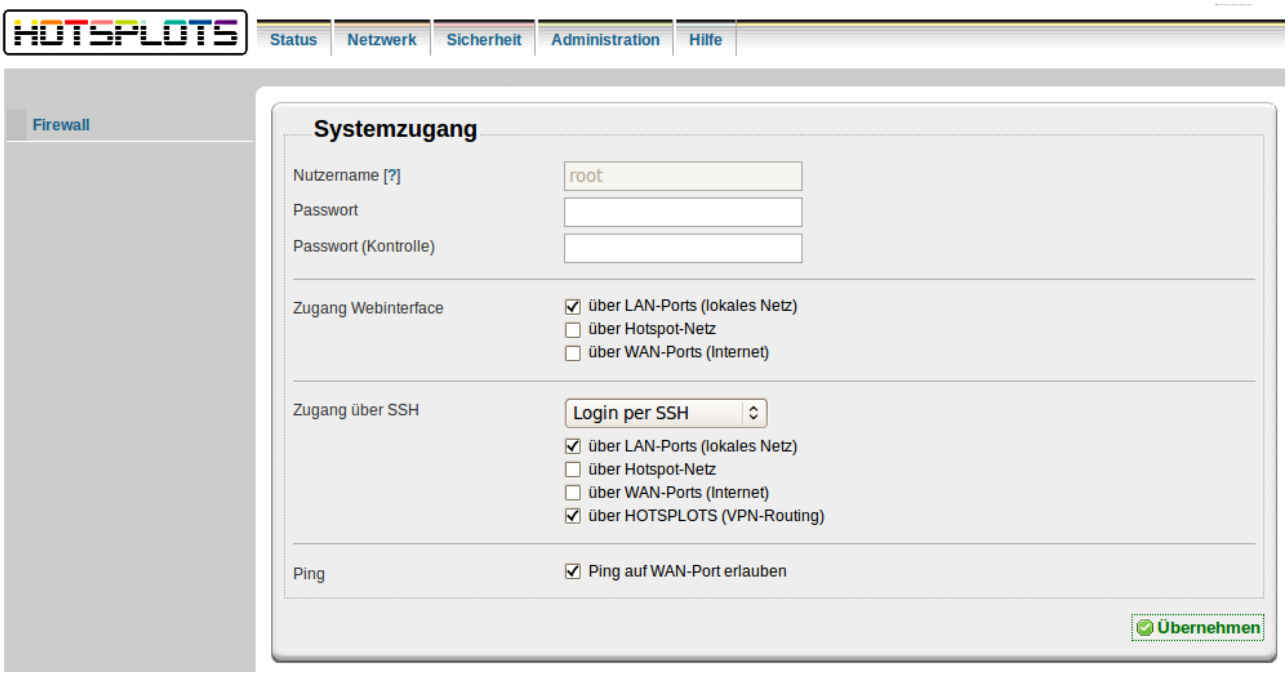


Abbildung 20: Einstellungen Sicherheit

Hier werden die möglichen Wege zur Administration des Gerätes und die Passwörter dafür gesetzt.

Im Auslieferungszustand ist der Zugriff auf das Webinterface nur über einen der LAN-Ports möglich. Username und Passwort sind **root** und **admin**. Aus Sicherheitsgründen sollte beides geändert werden. Zusätzlich kann der Zugriff auf das Webinterface über WLAN und über WAN, sprich aus dem Internet erlaubt werden. Beides ist auch mit einem schwierig zu erratendem Passwort nicht wirklich sicher, weil die Übertragung dieser Daten unverschlüsselt erfolgt. Einen sicheren, weil verschlüsselten Weg bietet eine Administration per ssh. Abbildung 19 zeigt die Einstellmöglichkeit unter dem Menüpunkt Sicherheit.

Ein weiterer Weg zur Administration führt über die Konsole. Dies ist allerdings nur Nutzern mit Grundkenntnissen in Linux zu empfehlen.

Firewall

Abbildung 21: Firewall

Mit den Einstellungen zu den **Portweiterleitungen** können Portweiterleitungen gesetzt werden. Dies ist z. B. für den Hotspot-Router sinnvoll um dahinter liegende Access-Points erreichen zu können.

Wenn Sie etwa die Regel **8282 TCP 192.168.1.2:8080** gesetzt haben und der Hotspot-Router am WAN-Port die IP-Adresse 1.2.3.4 und ein kabelgebundener Access Point die LAN-Adresse 192.168.1.2 hat, dann können Sie unter http://1.2.3.4:8282 das Webinterface des APs auf der 192.168.1.2 erreichen.

Im Fenster **Regeln für Hotspot-Clients** können Sie einzelne IP-Adressen, wie z.B. 192.168.1.100 oder ganze Netzwerke wie z.B. 192.168.1.0/24 eingeben. Diese IP-Adressen (oder Netzwerke) sind dann vom Hotspot-Netz aus erreichbar.

4.4 Administration

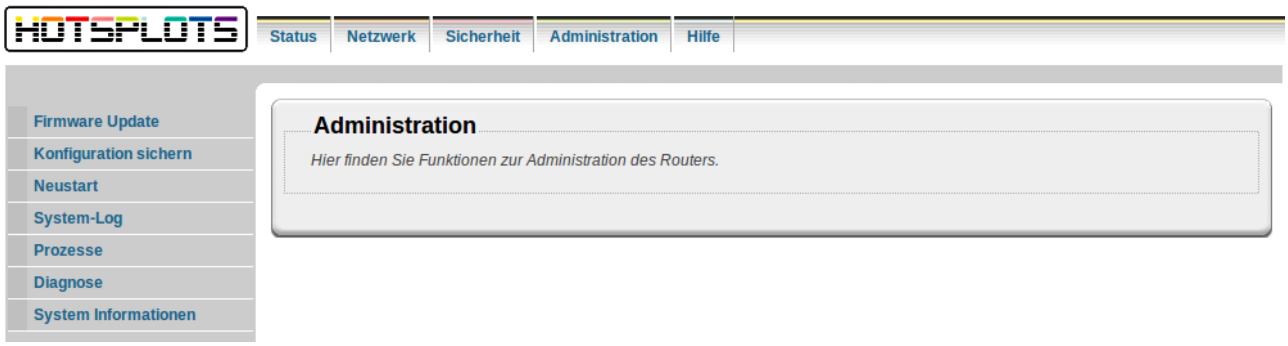


Abbildung 22: Einstellungen Administration

Firmware Update

Abbildung 23: Firmware-Update des Hotspot-Routers direkt über das Internet

Der einfachste Weg für ein Update der Firmware geht über den Button „von www.hotsplots.de flashen“. Dann verbindet sich der Router direkt mit dem Server von HOTSPLOTS und lädt die ausgewählte Version ohne Umweg über einen PC herunter – siehe Abbildung 23. Dies geht nur bei Hotspot-Routern, die über den WAN-Port mit dem Internet verbunden sind.

Alternativ können Sie die Firmware von http://www.hotsplots.de/support/files-links/firmware.html herunterladen, auf Ihrem PC zwischenspeichern und dann über den *Durchsuchen*-Button auf den Router

laden.

Konfiguration sichern

Unter diesem Menüpunkt können Sie über den Button **Konfiguration sichern** eine Datei vom Router herunterladen, die alle Konfigurationseinstellungen enthält. Diese Datei können Sie z.B. auf andere Geräte aufspielen (**Konfiguration wiederherstellen**), um Einstellungen zu duplizieren (z.B. für Access Points, aber Achtung: eindeutige IP-Adressen sind für APs notwendig), oder um Einstellungen im Fall eines „Verbastelns“ wieder herzustellen.

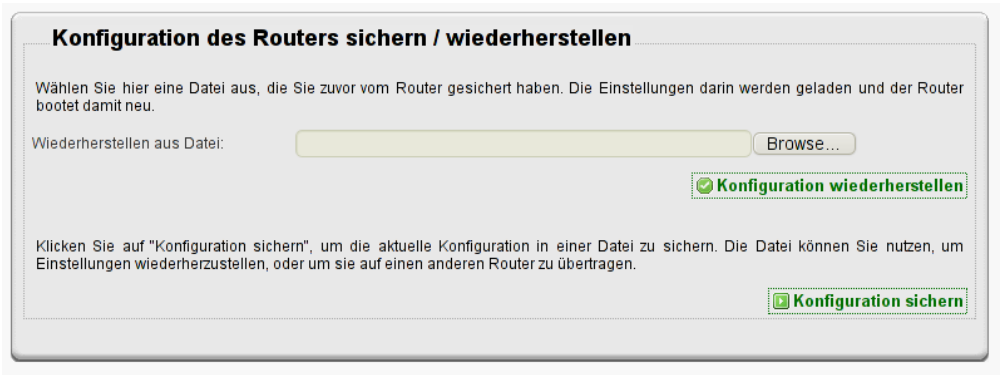


Abbildung 24: Konfiguration sichern

Neustart

Unter diesem Menüpunkt können Sie einen Neustart des Gerätes durchführen. Gespeicherte Einstellungen des Gerätes bleiben dabei erhalten. Je nach Gerätetyp dauert dieser Vorgang etwa eine Minute.

System-Log

An dieser Stelle sehen Sie alle Ereignisse, welche in der Logdatei des Routers enthalten sind. Erfahrene Anwender haben anhand des System-Logs die Möglichkeit, eventuelle Fehlerursachen oder Fehlkonfigurationen zu erkennen.

Prozesse

Alle Systemprozesse werden unter diesem Menüpunkt dargestellt. Außerdem können Sie ablesen, welche CPU- und Speicherauslastung die einzelnen Systemprozesse verursachen.

Diagnose

Es besteht die Möglichkeit, die Konfigurationseinstellungen des Gerätes an HOTSPLOTS zu senden. Hierbei werden die Konfigurationseinstellungen wie in der Funktion „Konfiguration sichern“ nicht nur lokal exportiert, sondern stehen den Technikern von HOTSPLOTS zur Verfügung. Dies ermöglicht im Fall der Fälle die schnelle Konfiguration eines Austauschgerätes.

System Information

Netzwerk- und Geräte-relevante Daten sind unter diesem Menüpunkt vermerkt. Unter anderem sehen Sie die im Gerät hinterlegten statischen Routen, die Bridgeinformationen sowie eine Liste aller Interfaces.

5 Administration über ssh

Dieser Weg der Administration ist nur für Fachleute mit Linux-Kenntnissen zu empfehlen und auch dann nur unter besonderen Umständen sinnvoll, z. B. Fernwartung komplexer Netzwerke, Skripten, o. ä. Detaillierte

Informationen sind unter www.openwrt.org zu finden, aber wir haben keine Idee, warum Sie zum Betrieb eines Hotspots darauf zurückgreifen sollten. Bevor Sie tief im System herumwerkeln, sprechen Sie mit uns! Wir empfehlen, nach Möglichkeit die Administration über das HOTSPLOTS-spezifische Web-Interface vorzunehmen.

5.1 Nützliche Linux-Befehle:

ifconfig gibt eine Liste der aktiven Netzwerkdevices und deren Konfiguration (IP-Adressen, etc.) aus.

top gibt die aktuell laufenden Prozesse und die Systemlast aus.

uptime gibt aus, wie lange das Gerät schon durchläuft (seit dem letzten Neustart)

fping -g *[IP-Adresse]/[Subnet]* scannt das gesamte Subnetz auf aktive Geräte. Dies ist z.B. sinnvoll, wenn das Vorhandensein diverser Accesspoints im Netzwerk überprüft werden muss.

logread gibt das System-Log aus.

6 Troubleshooting / Fehlersuche

6.1 Die Administrationsoberfläche lässt sich nicht aufrufen

1. Überprüfen Sie die Verkabelung. Sind wirklich ein LAN-Port (und nicht der WAN-Port) des Routers mit dem PC verbunden?
2. Überprüfen Sie die Einstellungen der Netzwerkkarte des Admin-PCs (der Rechner, der per Kabel mit dem Router verbunden ist). Die Karte sollte mit einer IP-Adresse statisch konfiguriert sein. Wenn Sie ein LAN mit mehreren Netzwerkkarten, vielen Kabeln und Switches haben, trennen Sie alles bis auf die Stromversorgung, das Netzwerkkabel zwischen Hotspot-Router und Admin-PC und ggf. dem Kabel am WAN-Port des Routers.
   Wenn Sie meine, es sei alles in Ordnung, Sie aber dennoch nicht das Web-Interface aufrufen können, konfigurieren Sie die Netzwerkkarte des Admin-PCs, die mit dem Router verbunden ist auf die IP-Adresse 192.168.1.2.
3. Drücken Sie im laufenden Betrieb den Resetknopf des Routers für mindestens 8 Sekunden. Daraufhin wird der Router auf Standardeinstellungen zurückgesetzt und erhält am LAN-Port die IP-Adresse 192.168.1.1 (unabhängig vom Hersteller des Routers), so dass Sie das Web-Interface unter http://192.168.1.1:8080 aufrufen können.

6.2 Man sieht das WLAN, aber die Loginseite wird nicht angezeigt.

1. Dann hat vermutlich der Hotspot-Router keine Verbindung ins Internet. Rufen Sie das Web-Interface auf und überprüfen Sie die Einstellungen unter Netzwerk > WAN / Internetanbindung.
2. Eine zweite Ursache kann daran liegen, dass Ihre WLAN-Karte nicht korrekt konfiguriert ist. Die IP-Adresse muss per DHCP-Client, also automatisch bezogen werden. Die Loginseite wird nur dann dargestellt, wenn Sie auch über das Captive Portal (chilli) authentisiert sind. In der Regel sollten Sie eine IP-Adresse der Form 192.168.44.x erhalten.

6.3 Man kommt ohne Loginseite ins Internet

1. Sind Sie über einen der LAN-Ports mit dem Hotspot-Router verbunden? Dann arbeitet der Router vermutlich in der Betriebsart „Hotspot Router (ohne APs)“. Erkennbar daran, dass der Client keine IP-Adresse hat, die mit 192.168.44. beginnt.

2. Sind Sie vielleicht noch eingeloggt? Rufen Sie http://logout.hotsplots.de auf. Wenn da ein Button zum Ausloggen erscheint, war das der Grund.

7 Richtlinien zur Hotspot-Installation

7.1 IT-Sicherheit

Schutz des Hotspots vor unberechtigtem Zugriff

1. Sicheres Passwort für den Hotspot-Router setzen.
2. Sichere Passwörter für Access Points und Repeater setzen. Idealerweise hätte jedes Gerät ein eigenes Passwort. Wem das zu umständlich ist, der sollte zumindest für den Hotspot-Router ein anderes Passwort setzen als für die weiteren Netzknoten. Da auf dem Hotspot-Router das System für die Zugangskontrolle läuft, ist das Schadenspotential beim Hotspot-Router deutlich größer als etwa bei einem von vielen Access Points. Das Passwort für die APs und Repeater kann zudem mangels SSL-Verschlüsselung vergleichsweise einfach ausspioniert werden, wenn die Webadministration über Funkstrecken genutzt wird. Die sichere Alternative ist die Administration über ssh. Darüber lässt sich auch das Webinterface tunneln.
3. Die erlaubten Zugangswege für die Administration einschränken. Wenn der Hotspot-Router an einen DSL-Router und nicht an ein DSL-Modem angeschlossen wird, ist es empfehlenswert, dem Hotspot-Router eine statische WAN-IP zuzuweisen und die Administration über LAN und WLAN zu deaktivieren.

Schutz der Nutzer durch netzweite Client-Isolierung

Wenn mehrere Nutzer gleichzeitig im Netz angemeldet sind, besteht die Gefahr, dass ein Nutzer etwa auf ungeschützte Windows-Freigaben eines anderen Nutzers zugreifen kann.

Bei Access Points und Repeatern sollte die HOTSPLOTS Firmware ab Version 2.0-33 eingesetzt werden. Dann werden mit der Client-Isolierung, siehe Menüpunkt Netzwerk >> WLAN, alle Pakete mit einer Zieladresse in dem Adressbereich, in dem den Clients vom Hotspot-Router IP-Adressen zugewiesen werden, geblockt.

Wenn Access Points mit fremder Firmware eingesetzt werden, sollten die Geräte über Switche mit portbasierten VLANs isoliert werden. Gute Erfahrungen haben wir beispielsweise mit Linksys SLM224 oder SLM248 bzw. dem TP-Link SL2210WEB gemacht.

Schutz des vorhandenen Netzes vor Hotspot-Nutzern

Idealerweise wird der Hotspot über einen eigenen DSL-Anschluss, z.B. von HOTSPLOTS, versorgt.

Wenn der Hotspot denselben Internetanschluss nutzt wie z.B. das eigene Büronetz des Standortes, dann sollte die Firewall im Hotspot-Router dafür sorgen, dass Hotspot-Clients keinen Zugriff auf Rechner im lokalen Netz des Standortes haben:

Bei der Firmware 2.0 wird dies über vorformulierte Firewallregeln realisiert, die unter dem Menüpunkt Sicherheit >> Firewall / Ports aktiviert sein sollten. Ansonsten steht dort ein roter Warnhinweis.

Bei der Firmware 3.0 ist diese Firewall-Regel immer aktiv, sofern nicht ausdrücklich, manuell eine Regel für den Zugriff in ein lokales Netz definiert wird.

Idle-Timeout für Terminals

Automatische Logouts erfolgen nur, wenn das Guthaben aufgebraucht oder der Client nicht mehr erreichbar ist. Dies ist z.B. dann ein Problem, wenn vor Ort Terminals angeboten werden und Nutzer nicht daran denken, sich aktiv auszuloggen. Im Extremfall, z.B. eine Reha-Klinik, die Tickets mit einer Gültigkeit von drei Wochen ausgibt, könnte dies dazu führen, dass sich ein Gast mit einem neuen Ticket einloggt und dann drei Wochen lang alle Nutzer ohne erneutes Login mit der Kennung des Ersten surfen. Für solche Szenarien, kann HOTSPLOTS ein sogenanntes Idle-Timeout von z.B. 60 Sekunden eintragen. Dann würde ein Logout initiiert, sobald 60 Sekunden lang keine Daten von dem Client ins Internet übertragen werden. Damit das funktioniert, ist darauf zu achten, dass keine Hintergrundprozesse auf dem Terminal laufen, die zu oft auf das Internet zugreifen, z.B. um nach Updates zu fragen.

7.2 Physikalische Sicherheit

Zum einen sollte die Position der WLAN-Stationen unter dem Gesichtspunkt optimaler Funkverbindungen im zu versorgenden Bereich gewählt werden: also meist eine erhöhte Position über Möbeln, Menschen und anderen Absorbern, nicht zu dicht an metallischen Reflektoren oder abgeschirmt durch wasserhaltige Absorber (Holz, Lehm, Aquarien etc.).

Zum anderen sollte darauf geachtet werden, dass die Geräte soweit möglich vor **Diebstahl** und **Vandalismus** geschützt sind und elementare Gefährdungen möglichst reduziert werden. **Blitz**schutz spielt vor allem bei Outdoorgeräten ein wichtige Rolle. Antennen- und Netzwerkkabel, die in Dachnähe verlegt werden, müssen mit Blitzschutz versehen werden. Ggf. ist der vorhandene Blitzschutz von einer Fachfirma durch Fangstangen zu ergänzen.

Vor allem Indoor-Geräte sind gegenüber **Wasser** sehr empfindlich. Daher sollte der Einsatz in Feuchträumen und mögliches Eindringen von Wasser in das Gehäuse unbedingt vermieden werden

7.3 Entdecken von Störungen

Das **Monitoring**-System versendet automatisch per E-Mail sowohl Meldungen über eine Störung als auch über die Störungsbehebung. Dazu sollten im Kundenbereich auf hotsplots.de in den Eigenschaften des Hotspots im Feld „Admin Kontakt“ E-Mail-Adressen der zuständigen Stellen, z.B. Hotspot-Betreiber und Installationspartner, eingetragen sein und diese regelmäßig geprüft werden.

7.4 Beheben von Störungen

Sollte trotz aller Schutzmaßnahmen die Funktion des Hotspots gestört sein, ist es wichtig, dass die Störung so schnell wie möglich behoben wird. Dies ist nur möglich, wenn eine **aktuelle Dokumentation verfügbar** ist. Das heißt die Dokumentation muss erstens angelegt werden und zweitens jederzeit zugänglich hinterlegt werden. Die Person oder Firma, die die Installation des Hotspots vornimmt, sollte auch die Dokumentation anlegen. Im Sinne der Verfügbarkeit ist es optimal, wenn die Dokumentation sowohl **beim Installateur**, als auch b**eim Hotspot-Betreiber** sowie **bei HOTSPLOTS** hinterlegt ist. Dabei ist allerdings darauf zu achten, dass sichergestellt ist, dass die Dokumentation nicht in falsche Hände gerät.

Ab Firmware 3.0-16 können die Einstellungen des Hotspot-Routers automatisch an HOTSPLOTS übermittelt werden. Damit kann jederzeit und sehr schnell ein Ersatzgerät konfiguriert werden.

Ferner sollte die **Fernwartung für HOTSPLOTS** ermöglicht sein (Menüpunkt Sicherheit: „Zugang über SSH: über HOTSPLOTS (VPN-Routing)).

7.5 Maßnahmen zum Beenden des Hotspot-Angebotes

Falls der Hotspot später außer Betrieb genommen werden soll, informieren Sie bitte die Nutzer darüber. Der einfachste Weg ist, auf die Login-Seite einen kleinen Hinweistext zu setzen. Dort sieht es jeder regelmäßige

Nutzer und kann sich entsprechend darauf einstellen.

8 Anhang 1: Konfiguration eines Smart-Switches zur Trennung von APs mittels portbasierter VLANs

Access Points mit der Firmware von HOTSPLOTS unterstützen die Client-Isolierung. D.h. WLAN-Clients, die mit dem selben AP verbunden sind, sind vor gegenseitigem Zugriff z.B. auf Windows-Freigaben geschützt. Das ist jedoch ein Feature des WLAN-Treibers. In größeren Netzwerken mit über Switchen verbundenen APs oder Terminals ist der Treiber machtlos, wenn es darum geht, Clients die an verschiedenen APs bzw. Ports angeschlossen sind, vor gegenseitigem Zugriff zu schützen. Der einfachste Weg, hier für zusätzliche Sicherheit zu sorgen, ist entweder der Einsatz unserer Firmwares für APs, die die Firewall zur Trennung von Clients auch für gebrückte Netzwerke unterstützen, oder der Einsatz von Smart-Switchen, die portbasierte VLANs unterstützen.

Im Folgenden ist das Vorgehen für portbasierte VLANs am Beispiel des preiswerten TL-SL2210WEB von TP-Link mit insgesamt 10 Ports beschrieben.

Diesen Router bieten wir im Webshop an. Dort ist eine Konfigurationsdatei gespeichert, die die VLAN-Einstellungen enthält und per tftp, unter Windows z.B. mit Tftpd32 hochgeladen werden kann.

In Werkseinstellung ist der TL-SL2210WEB unter der IP-Adresse 192.168.0.1 zu erreichen - Nutzernamen und Passwort jeweils supervisor.

Unter dem Menüpunkt VLAN Setting > VLAN Mode "Port VLAN (Port-based VLAN)" auswählen.

Unter VLAN Setting > Port VLAN Setting oben nacheinander die VLANs 1 bis 8 auswählen und dann jeweils die Nummer des VLANs und GIGA und SFP auswählen.

Dies bewirkt, dass die Geräte oder Netze an den Ports 1 bis 8 nicht miteinander kommunizieren können, aber über alle über die Ports GIGA oder SFP erreicht werden können. An diese Ports kann das WAN und ggf. ein Rechner für die Wartung des LAN angeschlossen werden.

9 Impressum/Support/Kontakt

Offene Fragen oder auch Verbesserungsvorschläge senden Sie am besten per Mail an support@hotsplots.de.

Der technische Support ist zumindest werktags mindestens von 8:00 bis 20:00 zu erreichen:

Tel.: +49 (0)30 - 29 77 348-0
Fax: +49 (0)30 - 29 77 348-99

hotsplots GmbH
Rotherstr. 17
10245 Berlin

hotsplots GmbH, Berlin, Amtsgericht Charlottenburg HRB 93460B
Geschäftsführung: Dr. Ulrich Meier, Dr. Jörg Ontrup