

[Sammelthread] Die besten Terminal-Befehle

Beitrag von „Moorviper“ vom 16. September 2017, 00:11

Jaaaa Mann endlich nach Monaten ... irgendwas muss Apple heimlich gefixed haben / am tool wurde nichts gemacht.

Worum gehts airport-bssid
Was macht das:

Es ist ein fork/oder eine eigene Implementierung des airport Programmes fürs Terminal.

Wofür braucht man es:
In der Regel gar nicht 😄

Aber ab und zu dann doch:
Das Programm kann nicht nur Netze scannen sondern wie der Anhängsel schon andeutet gezielt auf eine bestimmte bssid connecten.

Habe das früher recht häufig im Freifunk Umfeld gebraucht um auf den richtigen Router zu kommen (haben ja alle die gleiche ssid)
Ebenso ist es praktisch an der Uni wenn das Client-steering dich mal wieder eine Etage höher auf den AP schubsen will dann connected man mit dem Tool bruteforce mäßig so lange auf den man will bis es klappt 😄

Bei Yosemite und El Capitan hat Apple viel am wlan stack und dns resolver gebastelt seit dem ging das tool nicht mehr :-/ man konnte scannen aber nicht mehr connecten.

Den Quelltext bekommt man hier:

Code

1. <https://github.com/qpSHiNqp/airport-bssid>

benutzt wird es zum connecten / zum scannen bssid und pw weg lassen.

Code

1. usage: sudo ./airport-bssid <ifname> [<bssid>] [<password>]

Ein Beispielscan:

Code

1. `sudo ./airport-bssid en0`
2. Notice: The interface en0 is in 802.11n phyMode.
3. ***** Scanned networks *****
4. ESSID, BSSID, Ch, RSSI(dBm)
5. Event-WLAN, b4:e9:b0:33:19:ad, 52, -82
6. Event-WLAN, 70:10:5c:93:ec:0d, 100, -89
7. Event-WLAN, 08:cc:68:0a:60:fd, 36, -57
8. Event-WLAN, 70:10:5c:db:87:4d, 100, -84
9. Event-WLAN, 08:cc:68:0a:ac:32, 6, -79
10. Event-WLAN, f0:29:29:0e:48:7d, 44, -85
11. Event-WLAN, 08:cc:68:0a:ac:3d, 64, -81
12. Event-WLAN, 08:cc:68:0a:60:f2, 11, -54
13. Event-WLAN, b4:e9:b0:33:19:a2, 6, -77
14. Event-WLAN, 70:10:5c:db:87:42, 1, -72
15. eduroam, b4:e9:b0:33:19:a1, 6, -77
16. eduroam, f0:29:29:92:23:0e, 132, -90
17. eduroam, 08:cc:68:0a:60:fe, 36, -56
18. eduroam, 70:10:5c:db:87:4e, 100, -84
19. eduroam, 08:cc:68:0a:ac:3e, 64, -81
20. eduroam, 08:cc:68:0a:ac:31, 6, -79
21. eduroam, b4:e9:b0:33:19:ae, 52, -80
22. eduroam, 08:cc:68:0a:60:f1, 11, -54
23. eduroam, 70:10:5c:db:87:41, 1, -73
24. *****
25. Network scan completed. If you want to connect to specific BSSID, please enter the command below:
26. `./airport-bssid <ifname> <bssid> [<password>]`

Alles anzeigen

Connecten mit Rückmeldung ist dann:

Code

1. `sudo ./airport-bssid en0 70:10:5c:db:87:4e`
2. Notice: The interface en0 is in 802.11n phyMode.
3. ***** Scanned networks *****
4. ESSID, BSSID, Ch, RSSI(dBm)
5. Event-WLAN, b4:e9:b0:33:19:ad, 52, -81
6. Event-WLAN, 70:10:5c:93:ec:0d, 100, -89
7. Event-WLAN, 08:cc:68:0a:60:fd, 36, -59

8. Event-WLAN, 70:10:5c:db:87:4d, 100, -85
9. Event-WLAN, 08:cc:68:0a:ac:32, 6, -80
10. Event-WLAN, f0:29:29:0e:48:7d, 44, -84
11. Event-WLAN, 08:cc:68:0a:ac:3d, 64, -83
12. Event-WLAN, 08:cc:68:0a:60:f2, 11, -55
13. Event-WLAN, b4:e9:b0:33:19:a2, 6, -76
14. Event-WLAN, 70:10:5c:db:87:42, 1, -74
15. eduroam, f0:29:29:0e:48:7e, 44, -84
16. eduroam, f0:29:29:92:23:0e, 132, -90
17. eduroam, 08:cc:68:0a:60:fe, 36, -59
18. [color=#008000]eduroam, 70:10:5c:db:87:4e, 100, -84[/color]
19. eduroam, 08:cc:68:0a:ac:3e, 64, -82
20. eduroam, 08:cc:68:0a:ac:31, 6, -79
21. eduroam, 08:cc:68:0a:60:f1, 11, -56
22. eduroam, 70:10:5c:db:87:41, 1, -72
23. *****
24. Associated to network "eduroam" (BSSID: 70:10:5c:db:87:4e)

Alles anzeigen

Gut die Colortags gehen im code natürlich nicht. Einfach grün vorstellen XD

Vielleicht kann es jemand gebrauchen 😄