

Wer bei IP-Fire den DHCP-Server für das blaue Netzwerk verwendet, muss unbedingt dazu auch die Option **DNS Update** aktivieren.

Anbei meine Einstellungen für ein Produktivsystem an einer Mittelschule:

Blue Interface	
Enabled:	<input checked="" type="checkbox"/>
Start address: *	<input type="text" value="192.168.200.10"/>
Deny known clients:	<input type="checkbox"/>
Default lease time (mins): *	<input type="text" value="600"/>
Domain name suffix:	<input type="text" value="localdomain"/>
Primary DNS: *	<input type="text" value="192.168.100.254"/>
Primary NTP server:	<input type="text"/>
Primary WINS server address:	<input type="text"/>
next-server:	<input type="text"/>
IP address:	192.168.200.1
Netmask:	255.255.252.0
End address: *	<input type="text" value="192.168.203.254"/>
Max lease time (mins): *	<input type="text" value="720"/>
Allow bootp clients:	<input type="checkbox"/>
Secondary DNS:	<input type="text"/>
Secondary NTP server:	<input type="text"/>
Secondary WINS server address:	<input type="text"/>
filename:	<input type="text"/>

* Required field Save

DNS Update

Enable DNS Update (RFC2136):

localdomain

Key Name: Secret: Algorithm: **HMAC-MD5** Save

Damit können ca. 1000 IP-Adressen vergeben werden. Die ersten 10 IP-Adressen verberge ich nicht.

Die blaue Karte hat folgende Einstellungen:

IP-Adresse: 192.168.200.1
Subnetz: 255.255.252.0
DNS-Server: 192.168.100.254

Die IP-Adresse bleibt 10 Stunden erhalten. Maximal 12 Stunden. Das sollte für einen ganzen Unterrichtstag reichen.

Mit dieser zusätzlichen Einstellung wird ein gravierendes DNS Problem behoben:

Unbound startet alle 2 bis 3 Minuten neu! Tausende Log-Einträge sind vermerkt. (Vermutlich wird das aber gar nicht bemerkt 😊)

Ein Blick in die Logs:

Logs – System Logs – Section: DNS Unbound

Log

Total hits for log section unbound February 26, 2024: **4538**

Log

Total hits for log section unbound February 22, 2024: **15123**

An folgenden Logeinträge sind die fehlerhaften Neustarts zu erkennen:

15:52:49	unbound: [3732:0]	info: start of service (unbound 119.0).
15:52:49	unbound: [3732:0]	notice: init module 1: iterator
15:52:49	unbound: [3732:0]	notice: init module 0: validator
15:52:49	unbound: [3732:0]	notice: Restart of unbound 119.0.

Folgende Einträge können ebenfalls vorkommen. Weitere Information dazu habe ich leider (noch) nicht. Diese kommen (ziemlich sicher) von den Ipad.

19:35:10	unbound: [3783:0]	info: validation failure <_dns.resolver.arpa. SVCB IN>: no DNSSEC records from 8.8.8.8 for DS resolver.arpa. while building chain of trust
19:22:28	unbound: [3783:0]	info: validation failure <_dns.resolver.arpa. SVCB IN>: no DNSSEC records from 8.8.8.8 for DS resolver.arpa. while building chain of trust

Ich interpretiere das so, dass das entsprechende Gerät beim Surfen keine durchgängige DNSSEC-Abfrage mit dem Google-DNS Server (8.8.8.8) zu einer Domain zu Stande gebracht hat. Ich nehme an, Apple hat da wieder mal was ungestellt.

26.2.2024

Martin