Paket DNS_DHCP - Hostnamen, DNS- und DHCP-Server sowie DHCP-Relay Version 3.10.18

Peter Schiefer
E-Mail: team@fli4l.de

Das fli4l-Team
E-Mail: team@fli4l.de

15. September 2019

Inhaltsverzeichnis

1 Dokumentation des Paketes DNS_DHCP

1.1 DNS_DHCP - DNS- und DHCP-Server sowie DHCP-Relay und Slave DNS Server

1.1.1 Hostnamen

Hosts

OPT_HOSTS Mit der optionalen Variable `OPT_HOSTS` kann die Konfiguration von Hostname deaktiviert werden!

HOST_N HOST_x_{attribute} Es sollten alle Rechner im LAN beschrieben werden - mit IP-Adresse, Namen, Aliasnamen und evtl. Mac-Adressen für die dhcp-Konfiguration . Dazu setzt man zunächst die Anzahl der Rechner mit der Variablen `HOST_N`.

Hinweis: Seit Version 3.4.0 wird der Eintrag für den Router aus den Angaben in der `<config>/base.txt` generiert. Sollen zusätzliche Aliasnamen aufgenommen werden, siehe auch `HOSTNAME_ALIAS_N` (Seite **??**).

Anschließend werden mit den Attributen die Eigenschaften des Hostes definiert. Dabei sind einige Attribute Pflicht, wie z.B. IP-Adresse und Name, die anderen optional, d.h. man kann, aber man muß sie nicht spezifizieren.

NAME – Name des n-ten Hostes

IP4 – IP-Adresse (ipv4) des n-ten Hostes

IP6 – IP-Adresse (ipv6) des n-ten Hostes (optional). Wenn man "auto" verwendet, dann wird die Adresse bei aktiviertem OPT_IPV6 aus einem IPv6-Präfix (mit /64er-Netzmaske) und der MAC-Adresse des jeweiligen Hosts automatisch berechnet. Damit das funktioniert, muss die MAC-Adresse via `HOST_x_MAC` gesetzt (siehe unten) und das Paket `ipv6` entsprechend konfiguriert werden.

DOMAIN – DNS-Domain des n-ten Hostes (optional)

ALIAS_N – Anzahl der Alias-Namen des n-ten Hostes

ALIAS_m – m-ter Alias-Name für den n-ten Host

MAC – Mac Adresse des n-ten Hostes

DHCPTYP – Vergabe der IP-Adresse per DHCP abhängig von MAC oder NAME (optional)

In der Beispiel-Datei sind 4 Rechner konfiguriert - nämlich die PCs "client1", "client2", "client3" und "client4".

```
HOST_1_NAME='client1'                # 1st host: ip and name
HOST_1_IP4='192.168.6.1'
```

Aliasnamen müssen mit kompletter Domain angegeben werden.

Die MAC-Adresse ist optional und ist nur dann relevant, wenn fli4l zusätzlich als DHCP-Server eingesetzt wird. Dies wird in der Beschreibung zum optionalen Programmpaket "OPT_DHCP" erklärt, siehe unten. Ohne Einsatz als DHCP-Server sind lediglich die IP-Adresse, der Name des Rechners und eventuell Aliasnamen einzusetzen. Die MAC-Adresse ist eine 48-Bit-Adresse und besteht aus 6 Hex-Werten, welche durch einen Doppelpunkt voneinander getrennt werden, z.B.

```
HOST_2_MAC='de:ad:af:fe:07:19'
```

Hinweis: Wird fli4l um das IPv6-Paket ergänzt, brauchen keine IPv6-Adressen hinterlegt zu werden, wenn gleichzeitig die MAC-Adressen der Hosts vorliegen, weil das IPv6-Paket dann die IPv6-Adressen automatisch berechnet (modifiziertes EUI-64). Natürlich kann man aber den Automatismus unterbinden und feste IPv6-Adressen vorgeben, wenn man dies wünscht.

Extra Hosts

HOST_EXTRA_N HOST_EXTRA_x_NAME HOST_EXTRA_x_IP4 HOST_EXTRA_x_IP6
Mit diesen Variablen können weitere Hosts hinzugefügt werden die nicht der lokalen Domain angehören wie z.b. Hosts die sich auf der anderen Seite eines VPNs befinden.

1.1.2 DNS-Server

OPT_DNS Um den DNS-Server zu aktivieren ist die Variable OPT_DNS mit 'yes' zu belegen.

Werden im LAN keine Windows-Rechner verwendet oder ist bereits ein DNS-Server vorhanden, kann man OPT_DNS auf 'no' setzen und den Rest in diesem Abschnitt übergehen.

Im Zweifel immer (Standard-Einstellung): OPT_DNS='yes'

Allgemeine DNS-Optionen

DNS_LISTEN_N DNS_LISTEN_x Wenn Sie OPT_DNS='yes' gewählt haben, können Sie mit Hilfe von DNS_LISTEN_N die Anzahl, und mit DNS_LISTEN_1 bis DNS_LISTEN_N lokale IPs angeben, auf denen dnsmasq DNS-Anfragen annehmen darf. Sollten Sie bei DNS_LISTEN_N eine 0 eingetragen haben, beantwortet dnsmasq DNS-Anfragen auf allen lokalen IPs. An dieser Stelle dürfen nur IPs von existierenden Schnittstellen (ethernet, wlan ...) verwendet werden, es kommt sonst zu Warnmeldungen beim Start des Routers. Alternativ ist nun möglich hier auch ALIAS-Namen zu verwenden, z. B. IP_NET_1_IPADDR

Für alle hier angegebenen Adressen werden bei PF_INPUT_ACCEPT_DEF='yes' und/oder PF6_INPUT_ACCEPT_DEF='yes' entsprechende ACCEPT-Regeln in der INPUT-Kette der Firewall erzeugt. Im Falle DNS_LISTEN='0' werden ebenfalls Regeln erzeugt, die den DNS-Zugriff auf *allen* konfigurierten Schnittstellen erlauben.

Wichtig: *Falls der DNS-Server auf zur Laufzeit dynamisch hinzugefügten Schnittstellen horchen soll, etwa auf Netzwerk-Schnittstellen von VPN-Tunneln, sollten Sie dieses Array leer lassen, da andernfalls der DNS-Server nicht auf DNS-Anfragen antworten wird, die über den VPN-Tunnel gestellt werden.*

Im Zweifelsfalle können die Standardeinstellungen übernommen werden.

DNS_BIND_INTERFACES Falls Sie den DNS-Server via `DNS_LISTEN_x` nur an bestimmte Adressen binden möchten *und* zusätzlich einen *weiteren* DNS-Server an *andere* Adressen binden möchten, können Sie durch diese Option den DNS-Server anweisen, sich auch wirklich *nur* an die gelisteten Adressen zu binden. Standardmäßig bindet sich der DNS-Server an *alle* Schnittstellen und wirft bei Adressen im `DNS_LISTEN_x`-Array DNS-Anfragen, die an nicht konfigurierten Adressen ankommen, weg. Dies hat den Vorteil, dass der DNS-Server auch mit zur Laufzeit dynamisch hinzugefügten Schnittstellen umgehen kann, aber den Nachteil, dass kein alternativer DNS-Server auf dem Standard-DNS-Port 53 gleichzeitig laufen kann. Ein Anwendungsfall für einen zweiten DNS-Server ist, wenn Sie einen Slave-DNS-Server wie "yadifa" direkt auf dem fli4l-Router betreiben möchten. Soll also der dnsmasq nicht exklusiv auf dem fli4l eingesetzt werden, muss die Einstellung 'yes' gewählt und die für den dnsmasq zu nutzenden IP-Adressen per `DNS_LISTEN` konfiguriert werden.

DNS_VERBOSE Logging von DNS-Queries: 'yes' oder 'no'

Für ausführlichere Ausgaben des DNS, muß `DNS_VERBOSE` auf yes gesetzt werden. In diesem Fall werden DNS-Anfragen an den Nameserver protokolliert - und zwar über die syslog-Schnittstelle. Damit die Ausgaben auch sichtbar werden, ist dann auch die Variable `OPT_SYSLOGD='yes'` (Seite **??**) zu setzen, s.u.

DNS_MX_SERVER Mit dieser Variable gibt man hier den Hostnamen für den MX-Record (Mail-Exchanger) für die in `DOMAIN_NAME` definierte Domain an. Ein MTA (Mail-Transport-Agent, wie z.B. sendmail) auf einem internen Server fragt per DNS nach einem Mail-Exchanger für die Zieldomain der zuzustellenden Mail. Der DNS-Server liefert hiermit dem MTA den entsprechenden Host, der für Mails der Domain `DOMAIN_NAME` zuständig ist.

Dies ist keine automatische Konfiguration für Mail-Clients, wie z.B. Outlook! Also bitte nicht gmx.de hier eintragen und dann wundern, warum Outlook nicht funktioniert.

DNS_FORBIDDEN_N DNS_FORBIDDEN_x Hier können Sie Domains angeben, bei denen DNS-Queries vom DNS-Server prinzipiell als "nicht vorhanden" beantwortet werden sollen.

Beispiel:

```
DNS_FORBIDDEN_N='1'
DNS_FORBIDDEN_1='foo.bar'
```

In diesem Fall wird zum Beispiel eine Anfrage nach www.foo.bar mit einem Fehler beantwortet.

Man kann damit auch ganze Top-Level-Domains verbieten:

```
DNS_FORBIDDEN_1='de'
```

Dann ist die Namensauflösung für sämtliche Rechner in der DE-Topleveldomain abgeschaltet.

DNS_REDIRECT_N DNS_REDIRECT_x DNS_REDIRECT_x_IP Hier können Domains angegeben werden, bei welchen DNS-Queries vom DNS-Server auf eine spezielle IP umgeleitet werden.

Beispiel:

```
DNS_REDIRECT_N='1'
DNS_REDIRECT_1='yourdom.dyndns.org'
DNS_REDIRECT_1_IP='192.168.6.200'
```

In diesem Fall wird zum Beispiel eine Anfrage nach yourdom.dyndns.org mit der IP 192.168.6.200 beantwortet. Somit kann man externe Domains auf andere IPs umleiten.

DNS_BOGUS_PRIV Setzt man diese Variable auf ‘yes‘, werden reverse-lookups für IP-Adressen nach RFC1918 (Private Address Bereiche) nicht vom dnsmasq an andere DNS-Server weitergeleitet, sondern vom dnsmasq beantwortet.

DNS_FORWARD_PRIV_N DNS_FORWARD_PRIV_x Gelegentlich möchte man trotz aktiviertem `DNS_BOGUS_PRIV` die Auflösung von Adressen einiger privater Subnetze dennoch an die konfigurierten DNS-Server delegieren. Dies ist zum Beispiel nötig, wenn ein Uplink-Router private Subnetze verwaltet. Diese Array-Variable kann dafür genutzt werden, die privaten Subnetze zu benennen, deren Auflösung delegiert werden darf.

DNS_FILTERWIN2K Setzt man diese Variable auf ’yes’, werden DNS-Anfragen vom Typ SOA, SRV und ANY geblockt. Dienste, die diese Anfragen verwenden, werden dann nicht mehr ohne weitere Konfiguration funktionieren.
Dazu zählen zum Beispiel:

- XMPP (Jabber)
- SIP
- LDAP
- Kerberos
- Teamspeak3 (seit Client-Version 3.0.8)
- Minecraft (seit Vollversion 1.3.1)
- Ermittlung des Domänencontrollers (Win2k)

Siehe hierzu auch:

- Generelle Erklärung der DNS Record Arten:
  http://en.wikipedia.org/wiki/List_of_DNS_record_types
- Manpage von dnsmasq:
  http://www.thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html
- SRV-Record im Speziellen:
  http://de.wikipedia.org/wiki/SRV_Resource_Record

Durch Setzen von 'no' können durch die zusätzlichen weitergeleiteten DNS-Anfragen ungewollte Einwahlverbindungen aufgebaut oder bestehende nicht abgebaut werden. Insbesondere bei ISDN- und UMTS-Verbindungen können dadurch Mehrkosten entstehen. Sie müssen selbst abwägen, was für Sie wichtiger ist.

DNS_FORWARD_LOCAL setzt man diese Variable auf 'yes' kann der fli4l-Router in einer Domäne mit DOMAIN_NAME='example.local' konfiguriert werden, die wiederrum per DNS_ZONE_DELEGATION_x_DOMAIN='example.local' von einem anderen Nameserver aufgelöst wird.

DNS_LOCAL_HOST_CACHE_TTL Gibt die TTL (Time to live, in Sekunden) für Einträge aus den /etc/hosts Dateien und den per DHCP vergebenen IP-Adressen an. Der Standardwert für den fli4l-Router beträgt 60 Sekunden. Standardmäßig setzt der dnsmasq die TTL für lokale Einträge auf 0 und deaktiviert damit faktisch das nachfolgende Caching der DNS Einträge. Die Idee dahinter ist das ablaufende DHCP Leases usw. zeitnah weitergegeben werden können. Fragt allerdings z.B. ein lokaler IMAP Proxy die DNS Einträge dadurch mehrfach pro Sekunde ab ist das eine deutliche Belastung für das Netzwerk. Ein Kompromiss ist daher ein relativ kurzer TTL von 60 Sekunden. Es kann ja auch ohne die kurze TTL von 60 Sekunden jederzeit zu einem simplen abschalten eines Hosts kommen, so dass die abfragende Software sowieso mit nicht antwortetenden Hosts klarkommen muss.

DNS_SUPPORT_IPV6 (optional)

setzt man diese optionale Variable auf 'yes' wird die Unterstützung für IPV6- Adressen des DNS-Servers aktiviert.

DNS-Zonenkonfiguration

Der dnsmasq kann auch eine DNS-Domäne eigenständig verwalten, d.h. er ist "authoritativ" für diese Domäne. Dazu muss man zweierlei tun: Zum einen muss angegeben werden, welcher externe (!) DNS-Namensdienst auf den eigenen fli4l verweist und über welche Netzwerk-Schnittstelle dies passiert. Die Angabe der externen Referenz ist erforderlich, denn die Domäne, welche der fli4l verwaltet, ist ja immer eine Unterdomäne einer anderen Domäne.[1] Die Angabe der Schnittstelle ist wichtig, weil sich der dnsmasq dort "nach außen" anders verhält als auf den anderen Schnittstellen "nach innen": Nach außen beantwortet der dnsmasq niemals Anfragen für Namen außerhalb der konfigurierten eigenen Domäne. Nach innen funktioniert der dnsmasq natürlich auch als DNS-Relay ins Internet, damit die Auflösung von nicht-lokalen Namen funktioniert.

Zum anderen muss konfiguriert werden, welche Netze nach außen via Namensauflösung erreichbar sind. Hierbei sollten natürlich nur Netze mit öffentlichen IP-Adressen angegeben werden, denn über private Adressen können Hosts von außen ohnehin nicht erreicht werden.

Im Folgenden wird die Konfiguration an einem Beispiel beschrieben. Dieses Beispiel setzt das IPv6-Paket sowie ein öffentlich geroutetes IPv6-Präfix voraus; letzteres kann z.B. von einem 6in4-Tunnel-Provider wie Hurricane Electric bereitgestellt werden.

[1] Wir gehen hier mal davon aus, dass niemand einen fli4l als DNS-Rootserver verwendet...

DNS_AUTHORITATIVE Die Einstellung `DNS_AUTHORITATIVE='yes'` aktiviert den authoritativen Modus des dnsmasq. Dies reicht jedoch nicht aus, da weitere Angaben gemacht werden müssen (s.u.).

Standard-Einstellung: `DNS_AUTHORITATIVE='no'`

Beispiel: `DNS_AUTHORITATIVE='yes'`

DNS_AUTHORITATIVE_NS Mit dieser Variable wird der DNS-Name konfiguriert, über den auf den fli4l von außen mit Hilfe eines DNS-NS-Records verwiesen wird. Das kann auch ein DNS-Name sein, der zu einem Dynamic DNS-Dienst gehört.

Beispiel: `DNS_AUTHORITATIVE_NS='fli4l.noip.me'`

DNS_AUTHORITATIVE_IPADDR Mit dieser Variable wird konfiguriert, an welcher Adresse bzw. Schnittstelle der dnsmasq DNS-Anfragen für die eigene Domäne authoritativ beantwortet. Symbolische Namen wie `IP_NET_2_IPADDR` sind erlaubt. Der dnsmasq kann nur an *einer* Adresse/Schnittstelle authoritativ antworten.

Momentan können nur fest zugewiesene Adressen angegeben werden. Adressen, die sich erst durch eine Einwahl ergeben (z.B. mit Hilfe einer PPP-Verbindung), können nicht verwendet werden. Dies wird in einer späteren fli4l-Version korrigiert werden.

Wichtig: *Zu beachten ist, dass dies niemals eine Adresse/Schnittstelle sein darf, an der das eigene LAN hängt, weil sonst keine nicht-lokalen Namen mehr im LAN aufgelöst werden können!*

Beispiel: `DNS_AUTHORITATIVE_IPADDR='IP_NET_2_IPADDR'`

DNS_ZONE_NETWORK_N DNS_ZONE_NETWORK_x Hier werden die Netzadressen angegeben, für die der dnsmasq authoritativ die Namen auflösen soll. Dabei funktioniert sowohl die Vorwärts- (Name zu Adresse) als auch die Rückwärtsauflösung (Adresse zu Name).

Ein komplettes Beispiel:

```
DNS_AUTHORITATIVE='yes'
DNS_AUTHORITATIVE_NS='fli4l.noip.me'
DNS_AUTHORITATIVE_IPADDR='IP_NET_2_IPADDR' # Uplink hängt an eth1
DNS_ZONE_NETWORK_N='1'
DNS_ZONE_NETWORK_1='2001:db8:11:22::/64'   # lokales IPv6-LAN
```

Dabei wird angenommen, dass "2001:db8:11::/48" ein zu dem fli4l öffentlich geroutetes IPv6-Präfix ist und dass für das LAN das Subnetz 22 gewählt wurde.

DNS Zone Delegation

DNS_ZONE_DELEGATION_N DNS_ZONE_DELEGATION_x Es gibt besondere Situationen, wo die Angabe eines oder mehrerer DNS Server sinnvoll ist, z.B. bei Einsatz von fli4l im Intranet ohne Internetanschluss oder einem Mix von diesen (Intranet mit eigenem DNS Server und zusätzlich Internetanschluss).

Stellen wir uns folgendes Szenario vor:

- Circuit 1: Einwahl in das Internet
- Circuit 2: Einwahl in das Firmen-Netz 192.168.1.0 (firma.de)

Dann wird man `ISDN_CIRC_1_ROUTE` auf '0.0.0.0' und `ISDN_CIRC_2_ROUTE` auf '192.168.1.0' setzen. Bei Zugriff auf Rechner mit IP-Adresse 192.168.1.x wird fli4l dann den Circuit 2, sonst den Circuit 1 benutzen. Wenn das Firmennetz aber nicht öffentlich ist, wird in diesem vermutlich ein eigener DNS Server betrieben. Nehmen wir an, die Adresse dieses DNS Servers wäre 192.168.1.12 und der Domainname wäre "firma.de".

In diesem Fall gibt man an:

```
DNS_ZONE_DELEGATION_N='1'
DNS_ZONE_DELEGATION_1_UPSTREAM_SERVER_N='1'
DNS_ZONE_DELEGATION_1_UPSTREAM_SERVER_1_IP='192.168.1.12'
DNS_ZONE_DELEGATION_1_DOMAIN_N='1'
DNS_ZONE_DELEGATION_1_DOMAIN_1='firma.de'
```

Dann werden bei DNS Anfragen an die Domain firma.de der firmeninterne DNS Server benutzt. Alle anderen DNS Anfragen gehen wie üblich an die DNS Server im Internet.

Ein anderer Fall:

- Circuit 1: Internet
- Circuit 2: Firmen-Netz 192.168.1.0 *mit* Internetanschluss

Hier hat man also die Möglichkeit, auf 2 Wegen in das Internet zu gelangen. Möchte man geschäftliches und privates trennen, bietet sich dann folgendes an:

```
ISDN_CIRC_1_ROUTE='0.0.0.0'
ISDN_CIRC_2_ROUTE='0.0.0.0'
```

Man legt also auf beide Circuits eine Defaultroute und schaltet dann die Route mit dem imond-Client um - je nach Wunsch. Auch in diesem Fall sollte man `DNS_ZONE_DELEGATION_N` und `DNS_ZONE_DELEGATION_x_DOMAIN_x` wie oben beschrieben einstellen.

Möchte man auch die Reverse-DNS-Auflösung für ein so erreichbares Netz nutzen, z.B. wird ein Reverselookup von einigen Mailserver gemacht, gibt man in der optionalen Variable `DNS_ZONE_DELEGATION_x_NETWORK_x`, das/die Netz(werke) an, für die der Reverselookup aktiviert werden soll. Das folgende Beispiel verdeutlicht das:

```
DNS_ZONE_DELEGATION_N='2'
DNS_ZONE_DELEGATION_1_UPSTREAM_SERVER_N='1'
DNS_ZONE_DELEGATION_1_UPSTREAM_SERVER_1_IP='192.168.1.12'
DNS_ZONE_DELEGATION_1_DOMAIN_N='1'
DNS_ZONE_DELEGATION_1_DOMAIN_1='firma.de'
DNS_ZONE_DELEGATION_1_NETWORK_N='1'
DNS_ZONE_DELEGATION_1_NETWORK_1='192.168.1.0/24'
DNS_ZONE_DELEGATION_2_UPSTREAM_SERVER_N='1'
DNS_ZONE_DELEGATION_2_UPSTREAM_SERVER_1_IP='192.168.2.12'
DNS_ZONE_DELEGATION_2_DOMAIN_N='1'
DNS_ZONE_DELEGATION_2_DOMAIN_1='bspfirma.de'
DNS_ZONE_DELEGATION_2_NETWORK_N='2'
DNS_ZONE_DELEGATION_2_NETWORK_1='192.168.2.0/24'
DNS_ZONE_DELEGATION_2_NETWORK_2='192.168.3.0/24'
```

Mit der Konfigurationsoption DNS_ZONE_DELEGATION_x_UPTREAM_SERVER_x_QUERYSOURCEIP kann man die IP-Adresse für die ausgehenden DNS Anfragen an den oder die Upstream DNS Server setzen. Das ist z.B. dann sinnvoll wenn man den Upstream DNS Server über ein VPN erreicht und nicht möchte, dass die lokale VPN Adresse vom fli4l-Router als Quell IP-Adresse beim Upstream DNS Server auftaucht. Ein anderer Anwendungsfall ist eine vom Upstream DNS Server aus gesehen nicht routebare IP-Adresse (die durch ein VPN Interface evtl. auftritt). Auch in diesem Fall ist es notwendig die vom dnsmasq benutzte ausgehende IP-Adresse fest auf eine vom fli4l-Router benutzte und vom Upstream DNS Server aus erreichbar IP-Adresse zu setzen.

```
DNS_ZONE_DELEGATION_N='1'
DNS_ZONE_DELEGATION_1_UPSTREAM_SERVER_N='1'
DNS_ZONE_DELEGATION_1_UPSTREAM_SERVER_1_IP='192.168.1.12'
DNS_ZONE_DELEGATION_1_UPSTREAM_SERVER_1_QUERYSOURCEIP='192.168.0.254'
DNS_ZONE_DELEGATION_1_DOMAIN_N='1'
DNS_ZONE_DELEGATION_1_DOMAIN_1='firma.de'
DNS_ZONE_DELEGATION_1_NETWORK_N='1'
DNS_ZONE_DELEGATION_1_NETWORK_1='192.168.1.0/24'
```

DNS_REBINDOK_N DNS_REBINDOK_x_DOMAIN Der Nameserver *dnsmasq* lehnt normalerweise Antworten anderer Nameserver ab, die IP-Adressen aus privaten Netzwerken enthalten. Er verhindert dadurch eine bestimmte Klasse von Angriffen auf das Netzwerk. Hat man allerdings eine Domain in einem Netzwerk mit privaten IP-Adressen und einen extra Nameserver, der für dieses Netz zuständig ist, liefert der genau die Antworten, die vom *dnsmasq* abgelehnt werden würden. Diese Domains kann man in DNS_REBINDOK_x auflisten, die entsprechenden Antworten auf Anfragen zu der Domain werden dann akzeptiert. Ein weiteres Beispiel für Nameserver, die private IP-Adressen als Antwort liefern, sind sogenannte "Real-Time Blacklist Server". Ein Beispiel basierend auf diesen könnte wie folgt aussehen:

```
DNS_REBINDOK_N='8'
DNS_REBINDOK_1_DOMAIN='rfc-ignorant.org'
DNS_REBINDOK_2_DOMAIN='spamhaus.org'
DNS_REBINDOK_3_DOMAIN='ix.dnsbl.manitu.net'
DNS_REBINDOK_4_DOMAIN='multi.surbl.org'
DNS_REBINDOK_5_DOMAIN='list.dnswl.org'
DNS_REBINDOK_6_DOMAIN='bb.barracudacentral.org'
DNS_REBINDOK_7_DOMAIN='dnsbl.sorbs.net'
DNS_REBINDOK_8_DOMAIN='nospam.login-solutions.de'
```

1.1.3 DHCP-Server

OPT_DHCP Mit OPT_DHCP kann man einstellen, ob der DHCP-Server aktiviert wird.

DHCP_TYPE (optional)

Mit dieser Variable legt man fest, ob man die interne DHCP-Funktion des dnsmasq benutzt, oder ob man auf den externen ISC-DHCPD zurückgreifen will. Im Falle des ISC-DHCPD entfällt der Support für DDNS.

DHCP_VERBOSE aktiviert zusätzliche DHCP-Ausgaben im log.

DHCP_LS_TIME_DYN legt die standard Lease-Time für dynamisch vergebene IP-Adressen fest.

DHCP_MAX_LS_TIME_DYN legt die maximale Lease-Time für dynamisch vergebene IP-Adressen fest.

DHCP_LS_TIME_FIX Standard Lease-Time für statisch zugeordnete IP-Adressen.

DHCP_MAX_LS_TIME_FIX legt die maximale Lease-Time für statisch zugeordnete IP-Adressen fest.

DHCP_LEASES_DIR legt das Verzeichnis für die Leases-Datei fest. Möglich ist die Angabe eines absoluten Pfades oder des Wertes *auto*. Bei Angabe von *auto* wird die lease-Datei im Unterverzeichnis dhcp des persistent-Verzeichnisses (siehe Base-Dokumentation) abgelegt.

DHCP_LEASES_VOLATILE Befindet sich das Verzeichnis für die *Leases* in der Ram-Disk (da der Router z.B. von CD oder einem anderen nicht schreibbaren Medium bootet), gibt der Router beim Booten eine Warnung wegen einer fehlenden *Lease*-Datei aus. Diese Warnung entfällt, wenn man `DHCP_LEASES_VOLATILE` auf *yes* setzt.

DHCP_WINSSERVER_1 legt die Adresse des ersten WINS-Server fest. Bei installiertem und aktiviertem WINS-Server wird die Adresse des WINS-Server des SAMBA-Paketes übernommen.

DHCP_WINSSERVER_2 legt die Adresse des zweiten WINS-Server fest. Bei installiertem und aktiviertem WINS-Server wird die Adresse von WINS-Server des SAMBA-Paketes übernommen.

Lokale DHCP-Range

DHCP_RANGE_N Anzahl der DHCP-Ranges

DHCP_RANGE_x_NET Referenz zu einem in `IP_NET_x` definiertem Netz

DHCP_RANGE_x_START legt die erste zu vergebende IP-Adresse fest.

DHCP_RANGE_x_END legt die letzte zu vergebende IP-Adresse fest. Die beiden Variablen `DHCP_RANGE_x_START` und `DHCP_RANGE_x_END` kann man auch leer lassen, es wird dann keine DHCP-Range angelegt und nur die weiteren Variablen genutzt, um einem Host der per MAC-Zuordnung seine DHCP-IP bezieht, die Werte der Variablen zu übergeben.

DHCP_RANGE_x_DNS_SERVER1 legt die Adresse des DNS-Server für DHCP-Hosts des Netzes fest. Diese Variable ist optional. Wird hier nichts eingetragen, oder die Variable einfach weggelassen, wird die IP-Adresse, des zugeordneten Netzes verwendet. Es ist auch möglich, diese Variable auf 'none' zu setzen. Dann wird kein DNS-Server übertragen.

DHCP_RANGE_x_DNS_SERVER2 legt die IP-Adresse des zweiten DNS-Servers fest. Es gelten die gleiche Option wie in der vorherigen Variable

DHCP_RANGE_x_DNS_DOMAIN legt eine spezielle DNS-Domain für DHCP-Hosts dieser Range fest. Diese Variable ist optional. Wird hier nichts eingetragen, oder die Variable einfach weggelassen, wird der Default DNS-Domain `DOMAIN_NAME` verwendet.

DHCP_RANGE_x_NTP_SERVER legt die Adresse des NTP-Servers für DHCP-Hosts dieser Range fest. Diese Variable ist optional. Wird hier nichts eingetragen, oder die Variable einfach weggelassen, wird die IP-Adresse des in `DHCP_RANGE_x_NET` referenzierten Netzes verwendet, wenn ein Zeitserverpaket auf dem Router aktiviert ist. Es ist auch möglich, diese Variable auf 'none' zu setzen. Dann wird kein NTP-Server übertragen.

DHCP_RANGE_x_GATEWAY legt die Adresse des Gateways für diese Range fest. Diese Variable ist optional. Wird hier nichts eingetragen, oder die Variable einfach weggelassen, wird die IP-Adresse des in `DHCP_RANGE_x_NET` referenzierten Netzes verwendet. Es ist auch möglich, diese Variable auf 'none' zu setzen. Dann wird kein Gatway übertragen.

DHCP_RANGE_x_MTU legt die MTU für Clients in diesem Range fest. Diese Variable ist optional.

DHCP_RANGE_x_OPTION_N gestattet die Angabe Nutzer-definierter Optionen für diesen Bereich. Die verfügbaren Optionen kann man dem Manual des dnsmasq entnehmen (`http://thekelleys.org.uk/dnsmasq/docs/dnsmasq.conf.example`). Sie werden ungeprüft übernommen, können also bei Fehlern zu Problemen mit dem DNS/DHCP-Server führen. Diese Variable ist optional.

Extra DHCP-Range

DHCP_EXTRA_RANGE_N legt die Anzahl von DHCP-Bereichen fest, die an nicht lokale Netze vergeben werden. Hierzu ist am Gateway zum entsprechenden Netz ein DHCP-Relay zu installieren.

DHCP_EXTRA_RANGE_x_START erste zu vergebende IP-Adresse.

DHCP_EXTRA_RANGE_x_END letzte zu vergebende IP-Adresse.

DHCP_EXTRA_RANGE_x_NETMASK Netzwerkmaske für diesen Bereich.

DHCP_EXTRA_RANGE_x_DNS_SERVER Adresse des DNS-Servers für diesen Bereich.

DHCP_EXTRA_RANGE_x_NTP_SERVER Adresse des NTP-Servers für diesen Bereich.

DHCP_EXTRA_RANGE_x_GATEWAY Adresse des Default-Gateway für diesen Bereich.

DHCP_EXTRA_RANGE_x_MTU legt die MTU für Clients in dieser Range fest. Diese Variable ist optional.

DHCP_EXTRA_RANGE_x_DEVICE Netzwerkinterface über den dieser Bereich erreicht wird.

Nicht zugelassene DHCP-Clients

DHCP_DENY_MAC_N Anzahl der MAC-Adressen von Host, dennen der Zugriff auf DHCP-Adressen verweigert wird.

DHCP_DENY_MAC_x MAC-Adresse des Hosts, dem der Zugriff auf DHCP-Adressen verweigert wird.

Unterstützung fürs Booten vom Netz

Der dnsmasq unterstützt Clients, die via Bootp/PXE übers Netz booten. Die dafür nötigen Informationen werden vom dnsmasq bereitgestellt und pro Subnetz und Host konfiguriert. Die dafür nötigen Variablen sind in den DHCP_RANGE_%- und HOST_%-Abschnitten untergebracht und beschreiben das zu bootende File (*_PXE_FILENAME), den Server, der dieses File bereitstellt (*_PXE_SERVERNAME und *_PXE_SERVERIP) und evtl. notwendige Optionen (*_PXE_OPTIONS). Weiterhin kann man den internen tftp-Server aktivieren, so dass das Booten komplett von dnsmasq unterstützt wird.

HOST_x_PXE_FILENAME DHCP_RANGE_x_PXE_FILENAME Hier wird das zu bootende Image angegeben. Im Falle von PXE wird hier der zu ladende pxe-Bootloader, wie z.B. pxegrub, pxelinux oder ein anderer passender Bootloader angegeben.

HOST_x_PXE_SERVERNAME HOST_x_PXE_SERVERIP DHCP_RANGE_x_PXE_SERVERNAME Name und IP des tftp-Servers, werden diese Variablen leer gelassen, wird der Router selbst als tftp-Server übermittelt.

DHCP_RANGE_x_PXE_OPTIONS HOST_x_PXE_OPTIONS Einige Bootloader benötigen spezielle Optionen zum Booten. So erfragt zum Beispiel pxegrub über die Option 150 den Namen der Menu-Datei. Diese Optionen können hier angegeben werden und werden dann ins Konfigfile übernommen. Im Falle von pxegrub könnte das z.B. wie folgt aussehen:

```
HOST_x_PXE_OPTIONS='150,"(nd)/grub-menu.lst"'
```

Sind mehrere Optionen nötig, werden sie einfach mit Leerzeichen voneinander getrennt angegeben.

1.1.4 DHCP-Relay

Das DHCP-Relay wird dann verwendet, wenn ein anderer DHCP-Server die Verwaltung der Ranges übernimmt, der nicht direkt von den Clients erreicht werden kann.

OPT_DHCPRELAY Dieser Wert ist auf 'yes' zu setzen, damit der Router als DHCP-Relay arbeitet. Es darf nicht gleichzeitig ein DHCP-Server aktiv sein.

Standard-Einstellung: `OPT_DHCPRELAY`='no'

DHCPRELAY_SERVER An dieser Stelle wird der richtige DHCP-Server eingetragen, an den die Anfragen weitergereicht werden sollen.

DHCPRELAY_IF_N DHCPRELAY_IF_x Mit `DHCPRELAY_IF_N` gibt man die Anzahl der Netzwerkkarten an, auf denen der Relay-Server lauschen soll. In `DHCPRELAY_IF_x` werden dann die entsprechenden Netzwerkkarten angegeben.

Das Interface, über das die Antworten des DHCP-Servers wieder reinkommen, muß in der Liste mit aufgeführt werden.Zusätzlich muss sichergestellt werden, dass die Routen auf dem Rechner, auf dem der DHCP-Server läuft, korrekt gesetzt sind. Die Antwort des DHCP-Servers geht an die IP des Interfaces, an dem der DHCP-Client hängt. Nehmen wir folgendes Scenario an:

- Relay mit zwei Interfaces
- Interfaces zum Client: eth0, 192.168.6.1
- Interfaces zum DHCP-Server: eth1, 192.168.7.1
- DHCP-Server: 192.168.7.2

Dann muss es auf dem DHCP-Server eine Route geben, über den die Antworten an die 192.168.6.1 ihr Ziel erreichen. Ist der Router, auf dem das Relay läuft, der default gateway für den DHCP-Server, ist bereits alles ok. Ist dem nicht so, wird eine extra Route benötigt. Ist der DHCP-Server ein fli4l-Router, würde folgender Konfig-Eintrag dieses Ziel erreichen: IP_ROUTE_x='192.168.6.0/24 192.168.7.1'

Im Betrieb kann es zu Warnungen kommen, dass bestimmte Pakete ignoriert werden. Diese Warnungen kann man ignorieren, sie stören nicht den normalen Betrieb.

Beispiel:

```
OPT_DHCPRELAY='yes'
DHCPRELAY_SERVER='192.168.7.2'
DHCPRELAY_IF_N='2'
DHCPRELAY_IF_1='eth0'
DHCPRELAY_IF_2='eth1'
```

1.1.5 TFTP-Server

Der TFTP-Server wird dann verwendet, wenn der fli4l per TFTP Dateien ausliefern soll. Dies kann zum Beispiel dazu dienen, das ein Client per Netboot startet.

OPT_TFTP Aktiviert den internen TFTP-Server des dnsmasq. Standard-Wert ist 'no'.

TFTP_PATH Spezifiziert das Verzeichnis, in dem die Dateien liegen, die der tftp-Server an die Klienten ausliefern soll. Die entsprechenden Dateien sind mit Hilfe eines geeigneten Programms (z.B. scp) im entsprechenden Pfad abzulegen.

1.1.6 YADIFA - Slave DNS Server

OPT_YADIFA Aktiviert den YADIFA Slave DNS Server. Standard-Wert ist 'no'.

OPT_YADIFA_USE_DNSMASQ_ZONE_DELEGATION Wenn diese Einstellung aktiviert wird erzeugt das yadifa Startscript automatisch für alle Slavezonen entsprechende Zone Delegation Einträge für den dnsmasq. Damit sind die Slavezonen auch direkt über

den dnsmasq abfragbar und man benötigt im Prinzip keine YADIFA_LISTEN_x Einträge mehr. Die Anfragen werden dann vom dnsmasq beantwortet und einen nur auf localhost:35353 horchenden yadifa weitergeleitet.

YADIFA_LISTEN_N Wenn Sie `OPT_YADIFA`='yes' gewählt haben, können Sie mit Hilfe von `YADIFA_LISTEN_N` die Anzahl, und mit `YADIFA_LISTEN_1` bis `YADIFA_LISTEN_N` lokale IPs angeben, auf denen YADIFA DNS-Anfragen annehmen darf. Eine Portnummer ist optional möglich, mit der Angabe 192.168.1.1:5353 würde der YADIFA Slave DNS Server auf DNS Anfragen auf Port 5353 horchen. Achten Sie darauf, dass der dnsmasq in diesem Fall nicht auf allen Schnittstellen horchen darf (siehe `DNS_BIND_INTERFACES`). An dieser Stelle dürfen nur IPs von existierenden Schnittstellen (ethernet, wlan ...) verwendet werden, es kommt sonst zu Warnmeldungen beim Start des Routers. Alternativ ist nun möglich hier auch ALIAS-Namen zu verwende, z. B. `IP_NET_1_IPADDR`

YADIFA_ALLOW_QUERY_N

YADIFA_ALLOW_QUERY_x Gibt IP-Adressen und Netze an denen der Zugriff auf YADIFA erlaubt ist. YADIFA nutzt die Angaben um den fli4l Paketfilter entsprechend zu konfigurieren und die Konfigurationsdateien von YADIFA zu erstellen. Mit dem Prefix ! wird der IP-Adresse oder dem Netz der Zugriff auf YADIFA verweigert.

Der fli4l Paketfilter wird für YADIFA so konfiguriert, dass alle erlaubten Netze aus dieser Einstellung und der für die einzelnen Zonen zusammen in eine ipset Liste (yadifa-allow-query) aufgenommen werden. Eine Unterscheidung nach Zonen ist beim Paketfilter leider nicht möglich. Zusätzlich werden alle IP-Adressen und Netze aus dieser globalen Einstellung, denen der Zugriff verweigert wird, in diese Liste aufgenommen. Es ist daher nicht möglich den Zugriff später für einzelne Zonen wieder auszuweiten.

YADIFA_SLAVE_ZONE_N Gibt die Anzahl der Slave DNS Zonen an die YADIFA verwalten soll.

YADIFA_SLAVE_ZONE_x Der Name der Slave DNS Zone.

OPT_YADIFA_SLAVE_ZONE_USE_DNSMASQ_ZONE_DELEGATION Aktiviert ('yes') oder deaktiviert ('no') die dnsmasq Zone Delegation nur für die Slavezone.

YADIFA_SLAVE_ZONE_x_MASTER Die IP-Adresse mit einer optionalen Portnummer des DNS Master Server.

YADIFA_SLAVE_ZONE_x_ALLOW_QUERY_N

YADIFA_SLAVE_ZONE_x_ALLOW_QUERY_x Gibt IP-Adressen und Netze an denen der Zugriff auf diese YADIFA DNS Zone erlaubt ist. Damit kann der Zugriff auf bestimmte DNS Zonen weiter eingeschränkt werden. YADIFA nutzt die Angaben um die Konfigurationsdateien von YADIFA zu erstellen.

Mit dem Prefix ! wird die IP-Adresse oder das Netz der Zugriff auf YADIFA verweigert.

Abbildungsverzeichnis

Tabellenverzeichnis

Index