Paquetage DNS_DHCP - Nom d'hôte - Serveur DNS et DHCP - Relay DHCP Version 3.10.18

Peter Schiefer
courriel: team@fli4l.de

L'équipe fli4l
courriel: team@fli4l.de

15 septembre 2019

Table des matières

1 Documentation du paquetage DNS_DHCP

1.1 DNS_DHCP - Serveur DNS et DHCP - Relay DHCP et serveur DNS esclave

1.1.1 Nom d'hôte

Hôte

OPT_HOSTS Avec la variable optionnelle `opt_HOSTS`, vous pouvez désactiver la configuration des noms d'hôtes !

HOST_N HOST_x_{attribute} Tous les ordinateurs du réseau local doivent être enregistrés avec une adresse IP, un nom, un alias (ou pseudo) et éventuellement une adresse MAC pour la configuration du dhcpd. Pour ce faire, on indique d'abord le nombre d'ordinateur dans la variable `HOST_N`.

Remarque : depuis la version 3.4.0, l'enregistrement des informations du routeur sont générées dans le fichier `<config>/base.txt`. Des alias supplémentaires peuvent être ajoutés dans celui-ci, voir la variable `HOSTNAME_ALIAS_N` (Page **??**).

Ensuite on définit les caractéristiques de chaque hôte dans ces variables. certain paramètres sont obligatoires comme par ex. l'adresse IP, le nom et d'autres sont optionnels, c.-à-d. qu'ils ne sont pas obligatoires.

NAME – Nom d'hôte par n-fois

IP4 – Adresse IP (ipv4) de l'hôte par n-fois

IP6 – Adresse IP (ipv6) de l'hôte par n-fois (optionnelle) Si vous indiquez 'auto', l'adresse sera automatiquement composée du préfixe IPv6 (avec le masque de sous-réseau /64) et de l'adresse MAC correspondant à l'hôte si vous avez activé OPT_IPV6. Pour que cela fonctionne, vous devrez configurer `HOST_x_MAC` (voir ci-dessous) et configurer le paquetage `ipv6`.

DOMAIN – Domaine DNS de l'hôte par n-fois (optionnelle)

ALIAS_N – Nombre d'alias (ou pseudo)

ALIAS_m – m-fois le nom d'alias de l'hôte par n-fois

MAC – Adresse MAC de l'hôte par n-fois

MAC2 – Adresse MAC pour une autre interface de l'hôte par n-fois

DHCPTYP – Attribution de l'adresse IP par DHCP en fonction de l'adresse MAC ou du Nom (optionnelle)

Dans l'exemple du fichier dns_dhcp.txt, 4 ordinateurs sont configurés - Pour les PCs "client1", "client2", "client3" et "client4".

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

Les noms d'alias doivent être compatibles avec le nom complet du domaine spécifié dans fli4l.

L'adresse MAC est optionnelle, elle est pertinente que si fli4l utilise un serveur DHCP. Pour cela vous devez voir la description des options de la variable "OPT_DHCP" indiqué plus bas dans ce document. Si vous n'utilisez pas de serveur DHCP, vous pouvez juste indiquer l'adresse IP, le nom de l'ordinateur et peut-être un alias. L'adresse MAC à un adressage de 48 bits et se compose de 6 hexadécimales séparées par deux points.

Exemple :

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

Remarque : si vous ajoutez à fli4l le paquetage IPv6, il n'y a pas besoin d'indiquer les adresses IPv6, si l'adresse MAC est présente dans la configuration, le paquetage IPv6 créera automatiquement les adresses IPv6 (EUI-64 modifié) en utilisant l'adresse MAC. Bien sûr, vous n'êtes pas obligé d'utiliser l'adressage automatique, vous pouvez indiquer les adresses IPv6 manuellement sur l'hôte, si vous le souhaitez.

Extra hôte

HOST_EXTRA_N HOST_EXTRA_x_NAME HOST_EXTRA_x_IP4 HOST_EXTRA_x_IP6
Avec ces variables, vous pouvez ajouter d'autres hôtes qui n'appartiennent pas au domaine local, pas exemple des hôtes qui se trouvent sur un autre domaine à travers une connexion VPN

1.1.2 Serveur DNS

OPT_DNS Pour activer le serveur DNS vous devez paramétrer la variable OPT_DNS sur 'yes'. Si aucun ordinateur Windows n'est utilisé dans le LAN (ou réseau local), ou si un serveur DNS est déjà disponible dans le LAN, vous pouvez mettre la variable OPT_DNS sur 'no' et ignorer le reste de ce paragraphe.

Dans le doute, toujours utiliser la (configuration par défaut) : OPT_DNS='yes'

Option générale pour serveur DNS

DNS_LISTEN_N DNS_LISTEN_x Si vous avez choisi d'activer la variable OPT_DNS='yes', vous pouvez indiquer dans la variable DNS_LISTEN_N le nombre de variable à configurer et indiquez dans la variable DNS_LISTENIP_1 l'adresse IP locale sur laquelle, les requêtes DNS utiliserons le programme Dnsmasq. Si vous paramétrez la variable DNS_LISTEN_N sur '0' toutes les requêtes DNS des adresses IP locaux utiliserons le programme Dnsmasq.

À ce stade, seul les adresses IP des interfaces existantes (ethernet, wlan ...) peuvent être utilisées, sinon vous aurez un message d'avertissement au démarrage du routeur. Il est désormais possible d'utiliser alternativement les alias, par exemple IP_NET_1_IPADDR.

Pour toutes les adresses indiquées, les règles ACCEPT de la chaîne INPUT seront créées pour le pare-feu si PF_INPUT_ACCEPT_DEF='yes' et/ou PF6_INPUT_ACCEPT_DEF='yes' sont activées. Si la variable DNS_LISTEN='0' est à zéro, les règles qui permettent l'accès au DNS seront également générées pour *toutes* les interfaces configurées.

Important: *Si vous souhaitez que le serveur DNS écoute les interfaces configurées dynamiquement à l'installation, par exemple, une interface réseau pour un tunnel VPN. Vous*

ne devez pas configurer cette liste de variables, il faut les laisser vide. Sinon le serveur DNS ne répondra pas aux requêtes DNS effectuées via le tunnel VPN.

En cas de doute, vous pouvez utiliser les paramètres par défaut.

DNS_BIND_INTERFACES Si vous voulez que le serveur DNS écouter uniquement les adresses configurées via la variable `DNS_LISTEN_x` *et* si vous voulez un serveur DNS *supplémentaire* pour écouter les *autres* adresses du réseau. Avec cette option, vous demandez au serveur DNS d'écouter uniquement les adresses assignées. Par défaut, le serveur DNS écoute *toutes* les interfaces et envoie les requêtes DNS qui arrivent par les adresses qu'ils ne sont pas configurées dans la liste de variables `DNS_LISTEN_x`. Cette option a un avantage, c'est que le serveur DNS peut aussi traiter les interfaces configurées dynamiquement et un inconvénient c'est qu'aucun serveur DNS alternatif peut fonctionner simultanément en utilisant le port 53 du DNS standard. Si vous voulez utiliser le serveur DNS et si vous exécutez un deuxième serveur DNS esclave comme "yadifa" directement sur le routeur fli4l, vous devez savoir que le serveur Dnsmasq ne sera pas exclusivement utilisé par fli4l. Vous devez sélectionner le paramètre 'yes' et configurer les adresses IP dans la variable `DNS_LISTEN` pour pouvoir utiliser le serveur Dnsmasq.

DNS_VERBOSE Enregistrement des requêtes DNS : 'yes' ou 'no'

Si vous voulez avoir des détails sur les requêtes DNS, mettez la variable `DNS_VERBOSE` sur 'yes'. Dans ce cas, les messages des requêtes DNS seront consignés sur le serveur de nom - A savoir sur l'interface syslog. Si vous voulez rendre visible et lire ce fichier jounal, vous devez activer la variable `OPT_SYSLOGD='yes'` (Page **??**), voir ci-dessous.

DNS_MX_SERVER Avec cette variable, vous pouvez enregistrer un nom d'hôte pour le MX (Mail-Exchanger) et pour définir dans `DOMAIN_NAME` un domaine. Si un MTA (Mail"=Transport"=Agent, par exemple sendmail) est installé sur le serveur interne, une demande de DNS sera faite par Mail-Exchanger, l'objectif est d'envoyer un mail au domaine recherché. Le serveur DNS fournit ici l'hôte au MTA, pour l'envoi du mail au `DOMAIN_NAME` du domaine compétent.

Il ne s'agit pas de configuration automatique un clients de messagerie, comme par exemple Outlook ! Veuillez ne pas enregistrer votre adresse mail ici, après ne vous étonnez pas si Outlook ne fonctionne pas.

DNS_FORBIDDEN_N DNS_FORBIDDEN_x Avec ces variables, vous pouvez paramétrer les domaines pour lesquels les requêtes DNS n'auront "pas accés" au serveur DNS, ils n'auront aucune réponse.

Exemple :

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

Dans cet exemple une demande d'accés au domaine www.foo.bar répondra par une erreur.

On peut aussi interdire un Top-Level-Domains (ou domaines de premier niveau) les plus connus sont .com, .fr, .de :

```
DNS_FORBIDDEN_1='de'
```

Dans cet exemple, la résolution de nom pour 'de' du Top-level-domain sur le Web sera supprimé pour tous les ordinateurs du réseau local.

DNS_REDIRECT_N DNS_REDIRECT_x DNS_REDIRECT_x_IP Avec ces variables, vous pouvez spécifier les domaines sur lesquels les requêtes DNS seront redirigées vers une autre adresse IP du serveur DNS.

Exemple :

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

Dans cet exemple, une demande d'accés au domaine yourdom.dyndns.org sera dérivé vers l'adresse IP 192.168.6.200. Ainsi vous pouvez dériver les domaines externe de votre choix, sur une adresse IP local de votre choix.

DNS_BOGUS_PRIV Si vous placez cette variable sur 'yes' vous ne transmettez pas les recherches inversées pour les adresses IP RFC1918 (classe d'adresse IP privée, non routables sur Internet) ces adresses ne seront pas transmis au serveur DNS, mais le Dnsmasq répondra.

DNS_FORWARD_PRIV_N DNS_FORWARD_PRIV_x Si vous avez besoin de transmettre la résolution d'adresse de certain sous-réseau privés, malgré la configuration de la variable `DNS_BOGUS_PRIV` pour le serveur DNS. La transmission est nécessaire, par exemple si le routeur gère une connexion montante pour certain sous-réseaux privés. Cette ensemble de variables peut être utilisés pour définir les sous-réseaux privés, ainsi, la résolution d'adresse sera transmise.

DNS_FILTERWIN2K Si vous placez cette variable sur 'yes' les requêtes DNS du type SOA, SRV et ANY seront bloquées. Les services qui utilisent ce type de requète ne fonctionneront plus sans une configuration supplémentaire.

Par exemple :

— XMPP (Jabber)
— SIP
— LDAP
— Kerberos
— Teamspeak3 (à partir de la version du client 3.0.8)
— Minecraft (à partir de toutes les versions 1.3.1)
— Recherche pour la gestion du contrôleur de domaine (Win2k)

Pour plus d'informations :

— Voir les explications des types de requète DNS à cette adresse :
http://en.wikipedia.org/wiki/List_of_DNS_record_types
— Voir le manuel du Dnsmasq à cette adresse :
http://www.thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html
— Voir les requêtes SRV dans le détail à cette adresse :
http://en.wikipedia.org/wiki/SRV_resource_record

Si vous avez indiqué le paramètre 'no' en plus des problèmes de transmission des requêtes DNS, cela peut aussi provoquer des connexions indésirables ou empêcher la fermeture d'une connexion déjà existante. Surtout si vous utilisez l'ISDN (ou Numéris) ou l'UMTS, des coûts de connexion supplémentaires peuvent survenir. Vous devez choisir ce qui est le plus important pour vous.

DNS_FORWARD_LOCAL Si vous placez cette variable sur 'yes' le routeur fli4l peut être configuré dans un domaine avec la variable DOMAIN_NAME='example.local', et via

la variable DNS_ZONE_DELEGATION_x_DOMAIN='example.local' les requêtes seront résolues à partir d'un autre serveur de nom.

DNS_LOCAL_HOST_CACHE_TTL Vous indiquez dans cette variable le TTL (Time To Live, en seconde) pour les noms enregistrés dans le fichier /etc/hosts et pour les adresses IP affectés par le DHCP. La valeur par défaut pour fli4l est de 60 secondes. La valeur par défaut du TTL pour les noms enregistrés dans le Dnsmasq locale doit être de 0, en fait la mise en cache des entrées DNS sera désactivée. L'idée, est que l'exécution des baux du DHCP, etc. pourront être transmis rapidement. Exemple d'un Proxy IMAP local, il peut demander plusieurs fois par seconde un nom enregistré dans le DNS, cela occasionne des lourdes charges sur le réseau. Le compromis est donc un TTL relativement court, avec 60 secondes. Il peut même fonctionner sans ce court TTL de 60 secondes, avec une simple mise hors tension à tous moment de l'hôte, de sorte que le logiciel qui interroge ne traitera pas de toute façon la réponce de l'hote.

DNS_SUPPORT_IPV6 (optionelle)

Si vous placez cette variable sur 'yes' vous activez le serveur DNS supportant l'adressage IPv6.

Configuration d'une zone DNS

Le Dnsmasq peut également gérer un domaine DNS de manière autonome, c'est à dire, il a "autorité" pour ce domaine. Par conséquent, il faut faire deux choses : la première consiste à spécifier le nom du service DNS externe (!) sur fli4l pour l' envoie des requètes, la deuxième est savoir sur quelle interface réseau que tous cela se passera. La spécification du référencement externe est nécessaire, car le domaine qui gère fli4l, est toujours un sous-domaine d'un autre domaine. [1] La spécification de l'interface "externe" est important parce que Dnsmasq se comporte différemment par rapport à une autre interface "interne" : le Dnsmasq ne répond jamais aux requêtes de extérieur, en dehors de sa propre configuration de nom de domaine. En interne le Dnsmasq fonctionne naturellement comme un relay DNS pour que la résolution de noms qui n'est pas sur le routeur, fonctionne sur Internet.

D'autre part, vous devez configurer le réseau pour que la résolution de nom soit accessible vers l'extérieur. La configuration du réseaux ne doit être spécifiée avec une adresses IP publiques, parce que les adresses des hôtes privées, ne peuvent pas atteindre une IP publique qui est externe.

Ci-dessous, un exemple de configuration est décrite. Cet exemple suppose que le paquet IPv6 ainsi que le préfixe IPv6 est routé vers le réseau publique. Cette adresse peut par exemple, être fournis par le fournisseur de tunnel 6in4 comme Hurricane Electric.

DNS_AUTHORITATIVE Si vous activez la variable `DNS_AUTHORITATIVE='yes'`, vous activez le module Dnsmasq qui fait autorité. Toutefois, cela ne suffit pas, car vous devez fournir plus d'information (voir ci-dessous).

Paramètre par défaut :`DNS_AUTHORITATIVE='no'`

Exemple : `DNS_AUTHORITATIVE='yes'`

DNS_AUTHORITATIVE_NS Dans cette variable vous configurez le nom du DNS externe pour fli4l, vous indiquez ici le Nom de Domaine du DNS. Cela peut être un nom de DNS qui appartient à un service de DNS Dynamique.

1. Nous allons supposer que personne n'utilise fli4l comme serveur DNS à la racine...

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

DNS_AUTHORITATIVE_IPADDR Dans cette variable vous configurez l'adresse ou l'interface, sur la quelle les demandes de DNS du Dnsmasq doit répondre par le domaine qui fait autorité. Les noms symboliques comme `IP_NET_2_IPADDR` sont autorisés. Le Dnsmasq peut répondre seulement à *une* adresse/interface qui fait autorité.

Actuellement vous pouvez affecter seulement les adresses fixe. Les adresses qui sont produites par un accès à distance (par ex. en utilisant une connexion PPP), ne peut pas être utilisée. Ce problème sera résolu dans une version ultérieure de fli4l.

Important: *Il faut faire attention à se que l'adresse/interface ne dépend jamais du réseau local, autrement aucun nom ne sera résolu dans le LAN!*

Exemple : `DNS_AUTHORITATIVE_IPADDR='IP_NET_2_IPADDR'`

DNS_ZONE_NETWORK_N DNS_ZONE_NETWORK_x Dans cette variable vous configurez l'adresse réseau, pour que le Dnsmasq qui fait autorité puisse résoudre les noms. Il fonctionne à la fois en recherche normal (le nom de l'adresse IP) ainsi qu'en recherche inversée (l'adresse IP du nom).

Un exemple complet :

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

Il est supposé que "2001 :db8 :11 : :/48" est le réseau public et sera routé vers le préfix IPv6 dans fli4l, et que 22 sous-réseau dans le LAN ont été sélectionnés.

Délégation de zone DNS

DNS_ZONE_DELEGATION_N DNS_ZONE_DELEGATION_x Il y a des situations particulières, où le référencement d'un ou plusieurs serveurs DNS est utiliser, par exemple lorsque l'on utilise fli4l en Intranet sans connexion Internet ou un mélange des deux (un Intranet avec son propre serveur DNS et en plus une connexion Internet).

Si nous imaginons le scénario suivant :

— Circuit 1 : Avec une connexion Internet
— Circuit 2 : Avec une connexion à un réseau d'entreprises 192.168.1.0 nom de domaine (firma.de)

Nous allons configurer `ISDN_CIRC_1_ROUTE` sur '0.0.0.0' et `ISDN_CIRC_2_ROUTE` sur '192.168.1.0'. Pour accéder aux ordinateurs avec l'adresse IP 192.168.1.x fli4l utilisera le circuit 2, autrement le circuit 1 sera utilisé. Si le réseau d'entreprise n'est pas public, il est possible de mettre en service un serveur DNS interne dans le réseau. Supposons, que l'adresse de ce serveur DNS est 192.168.1.12 et le nom de domaine est "firma.de".

Vous devez alors paramétrer les variables suivantes :

```
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'
```

Aprés cette configuration, les requêtes DNS seront envoyées au domaine firma.de ils utiliseront le serveur DNS interne de l'entreprise. Tous les autres requêtes DNS iront comme d'usage vers un serveur DNS sur Internet.

Autre cas :

— Circuit 1 : Internet
— Circuit 2 : Réseau d'entreprise 192.168.1.0 *avec* une connexion Internet

Ici vous avez deux possibilités d'accéder à Internet. Si vous souhaitez séparer le travail et la vie privée, vous pouvez alors paramètrer :

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

Vous définissez donc les deux circuits avec une route par défaut et vous commutez alors les circuits en utilisant le client-imond - en fonction de la demande. Dans ce cas vous devez paramétrer les variables `DNS_ZONE_DELEGATION_N` et `DNS_ZONE_DELEGATION_x_DOMAIN_x` comme décrit ci-dessous.

Si vous voulez utiliser la résolution de DNS inversé sur votre réseau, par ex. faire une recherche inversée pour certains serveurs de messageries, vous pouvez indiquer dans la variable optionnelle `DNS_ZONE_DELEGATION_x_NETWORK_x`, le ou les réseaux (mis en oeuvres), cela active la recherche inversée. Voici un exemple :

```
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'
```

Avec l'option de configuration `DNS_ZONE_DELEGATION_x_UPTREAM_SERVER_x_QUERYSOURCEIP` vous pouvez définir l'adresse IP sortante qui interrogera le serveur DNS amont. C'est utile, par exemple quand vous allez sur le serveur amont via un VPN et si vous ne voulez pas que l'adresse locale du VPN fli4l apparaît comme l'adresse IP source dans le serveur amont. Autre cas d'application, l'adresse IP du serveur DNS amont ne sera pas routable (cela se produit éventuellement à travers une interface VPN). Dans autre cas, il est logique que le Dnsmasq utilise l'adresse IP sortante qui est paramétré sur le routeur fli4l et que l'adresse IP du serveur DNS amont soit défini pour être accessible.

```
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 Habituellement le serveur de noms *Dnsmasq* refuse de répondre à d'autre serveur de nom, s'il contient des adresses IP de réseau privé. Il empêche ainsi une certaine forme d'attaques réseau. Mais si vous avez un nom de domaine avec une adresse IP dans votre réseau et si un serveur de nom distinct responsable du réseau privé fournit les réponses exactes, il sera rejeté par le serveur *Dnsmasq*. On peut faire une liste de ces domaines dans la variable `DNS_REBINDOK_x`, les réponses appropriées des demandes au sujet de ce domaine, seront ensuite acceptées. Un autre exemple d'un serveur de nom qui fournirait les réponses aux adresses IP privées, ces serveurs sont soi-disant des "serveurs Blacklist en temps réel". Voici un exemple basé sur ces serveurs :

```
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 Serveur DHCP

OPT_DHCP Avec la variable `OPT_DHCP`, vous pouvez si vous le voulez activer un serveur DHCP.

DHCP_TYPE (optionnelle)

Avec cette variable, vous déterminez si vous voulez utiliser la fonction DHCP interne avec Dnsmasq, ou si vous voulez recourir à la fonction ISC-DHCPD externe. Dans ce cas avec ISC-DHCPD le support DDNS (ou DNS dynamique) sera supprimé.

DHCP_VERBOSE Avec cette variable, vous activez les messages sur les transactions DHCP dans le log (ou fichier journal).

DHCP_LS_TIME_DYN Avec cette variable, vous indiquez le Lease-Time (ou délai du bail) standard pour des adresses IP fournies dynamiquement.

DHCP_MAX_LS_TIME_DYN Avec cette variable, vous indiquez le Lease-Time (ou délai du bail) maximum pour des adresses IP fournies dynamiquement.

DHCP_LS_TIME_FIX Avec cette variable, vous indiquez le Lease-Time standard pour des adresses IP assignées statiquement.

DHCP_MAX_LS_TIME_FIX Avec cette variable, vous indiquez le Lease-Time maximum pour des adresses IP assignées statiquement.

DHCP_LEASES_DIR Avec cette variable, vous indiquez le répertoire pour le fichier du bail DHCP. Il est possible de spécifier un chemin absolu ou d'indiquer le paramètre *auto*. Si vous avez défini *auto* le fichier du bail sera stocké dans le sous-répertoire persistant du DHCP (voir la documentation de la Base)

DHCP_LEASES_VOLATILE Le répertoire *Leases* se trouve dans le disque RAM (car avec une installation par CD le routeur n'a pas autres supports), au boot le routeur enverra un message d'avertissement, à cause de l'absent du répertoire *Leases* pour l'installation des fichiers. Cet avertissement sera annulé, si vous indiquez dans la variable `DHCP_LEASES_VOLATILE` la valeur *yes*.

DHCP_WINSSERVER_1 Avec cette variable, vous indiquez l'adresse du premier serveur WINS. Le serveur WINS doit être installé et activé, l'adresse du serveur WINS est dans le paquetage SAMBA.

DHCP_WINSSERVER_2 Avec cette variable, vous indiquez l'adresse du deuxième serveur WINS. Le serveur WINS doit être installé et activé, l'adresse du serveur WINS est dans le paquetage SAMBA.

Plage DHCP locale

DHCP_RANGE_N Avec cette variable, vous indiquez le nombre de DHCP-Ranges (ou plage d'adresses IP).

DHCP_RANGE_x_NET Avec cette variable, vous indiquez le référencement du réseau défini dans la variable `IP_NET_x`.

DHCP_RANGE_x_START Avec cette variable, vous indiquez la première adresse IP.

DHCP_RANGE_x_END Avec cette variable, vous indiquez la dernière adresse IP. Les deux variables `DHCP_RANGE_x_START` et `DHCP_RANGE_x_END` peuvent aussi être laisser vide, alors, aucun DHCP-Range ne sera installé. Vous devez utiliser les autres variables, pour référence le DHCP-IP de l'hôte avec l'attribution d'une adresse MAC, pour pouvoir transmettre les valeurs de la variable.

DHCP_RANGE_x_DNS_SERVER1 Avec cette variable, vous définissez l'adresse IP du serveur DNS pour les hôtes du DHCP. Cette variable est optionnelle. Si rien n'est enregistré, la variable sera simplement omise et la variable utilisera l'adresse IP, associé au réseau. Il est également possible de placer 'none' dans cette variable, alors aucun serveur DNS ne sera utilisé.

DHCP_RANGE_x_DNS_SERVER2 Avec cette variable, vous définissez la seconde adresse IP du serveur DNS. Les options sont les même que dans la variable précédente.

DHCP_RANGE_x_DNS_DOMAIN Avec cette variable, vous définissez un domaine DNS spécifique pour les hôtes du DHCP de cette plage. Cette variable est optionnelle. Si rien n'est enregistré, la variable sera simplement omise et le domaine DNS par défaut `DOMAIN_NAME` sera utilisé.

DHCP_RANGE_x_NTP_SERVER Avec cette variable, vous définissez un serveur NTP spécifique pour les hôtes du DHCP de cette plage. Cette variable est optionnelle. Si rien n'est enregistré, la variable sera omise et l'adresse IP référencée dans la variable `DHCP_RANGE_x_NET` sera utilisée, pour les paquets du serveur de temps qui est activé sur le routeur. Il est également possible de placer 'none' dans cette variable, alors aucun serveur NTP ne sera utilisé.

DHCP_RANGE_x_GATEWAY Avec cette variable, vous définissez la Gateway (ou passerelle) pour les hôtes du DHCP de cette plage. Cette variable est optionnelle. Si rien n'est enregistré, la variable sera simplement omise et l'adresse IP référencée dans la variable `DHCP_RANGE_x_NET` sera utilisée. Il est également possible de placer 'none' dans cette variable, alors aucune Gateway ne sera utilisé.

DHCP_RANGE_x_MTU Avec cette variable, vous définissez la plage MTU du client. Cette variable est optionnelle.

DHCP_RANGE_x_OPTION_N Avec ces variables vous pouvez définir des options spécifiques pour ce domaine. Les options peuvent être trouvées dans le Manuel Dnsmasq (http://thekelleys.org.uk/dnsmasq/docs/dnsmasq.conf.example). Ces options n'ont pas été contrôlées, ils peuvent causer des erreurs ou des problèmes avec le serveur DNS/DHCP. Cette variable est optionnelle.

Extra plage DHCP

DHCP_EXTRA_RANGE_N Avec cette variable, vous indiquez le nombre de serveur DHCP qui ne sont pas dans le réseau local. Pour cela vous devez installer un relais DHCP qui sera sur le réseau de la gateway (ou passerelle).

DHCP_EXTRA_RANGE_x_START Avec cette variable, vous indiquez la première adresse IP.

DHCP_EXTRA_RANGE_x_END Avec cette variable, vous indiquez la dernière adresse IP.

DHCP_EXTRA_RANGE_x_NETMASK Avec cette variable, vous indiquez le masque de sous réseau.

DHCP_EXTRA_RANGE_x_DNS_SERVER Avec cette variable, vous indiquez l'adresse du serveur DNS pour ce domaine.

DHCP_EXTRA_RANGE_x_NTP_SERVER Avec cette variable, vous indiquez l'adresse du serveur NTP pour ce domaine.

DHCP_EXTRA_RANGE_x_GATEWAY Avec cette variable, vous indiquez l'adresse de la Gateway par défaut pour ce domaine.

DHCP_EXTRA_RANGE_x_MTU Avec cette variable, vous indiquez la plage MTU du client. Cette variable est optionnelle.

DHCP_EXTRA_RANGE_x_DEVICE Avec cette variable, vous indiquez l'interface réseau pour accéder à ce domaine.

Clients DHCP non autorisés

DHCP_DENY_MAC_N Avec cette variable, vous indiquez le nombre d'adresses MAC des hôtes, dont l'accès aux adresses du serveur DHCP sera refusé.

DHCP_DENY_MAC_x Avec cette variable, vous indiquez les adresses MAC des hôtes, dont l'accès aux adresses du serveur DHCP sera refusé.

Supporte le boot par le réseau

Dnsmasq supporte les clients, qui lancent le Bootp/PXE via le réseau pour booter (ou démarrer) fli4l. Les informations nécessaires sont fournies par le Dnsmasq pour configurer l'hôte sur le sous-réseau. Les variables nécessaires sont DHCP_RANGE_%- et HOST_%- Ce paragraphe décrit l'installation et le fichier de boot avec (*_PXE_FILENAME), le serveur met à disposition les variables (*_PXE_SERVERNAME et *_PXE_SERVERIP), éventuellement (*_PXE_OPTIONS) si nécessaire pour les options. De plus, on peut activer un serveur TFTP interne, si bien que le boot sera complètement supporté par Dnsmasq.

HOST_x_PXE_FILENAME DHCP_RANGE_x_PXE_FILENAME Avec cette variable, vous indiquez l'image boot à lancer. Avec PXE vous indiquez ici le pxe-Bootloader à charger, par exemple pxegrub, pxelinux ou un autre Bootloader qui convient.

HOST_x_PXE_SERVERNAME HOST_x_PXE_SERVERIP DHCP_RANGE_x_PXE_SERVERNAM Avec ces variables, vous indiquez Le nom et l'adresse IP du serveur TFTP, ces variables doivent rester vides, si le routeur est utilisé en tant que serveur TFTP.

DHCP_RANGE_x_PXE_OPTIONS HOST_x_PXE_OPTIONS Certains Bootloader ont besoin d'options pour booter. Il demande par exemple, avec pxegrub, l'option 150 avec le nom du fichier menu. Cette option peut être indiquer dans cette variable et sera reprise alors par le fichier config. Dans l'exemple pxegrub, on pourrait paramètrer comme ceci :

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

S'il est nécessaire d'indiquer plusieurs options, ils seront simplement séparés par un espace.

1.1.4 Relais DHCP

Le relais DHCP est utilisé, lorsqu'un autre serveur DHCP assume la gestion de la plage d'adresses IP et qui ne peut pas directement être atteint par les clients.

OPT_DHCPRELAY Vous devez paramétrer cette variable sur 'yes' pour que le routeur puisse faire fonctionner le relais DHCP. Il ne faut pas activer un serveur DHCP en même temps.

Configuration par défaut : `OPT_DHCPRELAY`='no'

DHCPRELAY_SERVER À ce stade, le serveur DHCP est correctement enregistré, pour que les demandes puissent passer.

DHCPRELAY_IF_N DHCPRELAY_IF_x Avec la variable `DHCPRELAY_IF_N`, on indique le nombre de cartes réseaux sur lesquelles le serveur Relay doit écouter. Dans la variable `DHCPRELAY_IF_x` on indique la carte réseau correspondantes.

L'interface sur laquelle le serveur DHCP répond aux demandes, doit être mentionnée dans la liste. En outre, il faut s'assurer que les routes de l'ordinateur, sur lequel le serveur DHCP est installé fonctionne correctement. La réponse du serveur DHCP doit provenir via l'adresse IP de l'interface sur laquelle le client DHCP dépend. Prenons le scénario suivant :

— Relais sur deux interfaces
— Interface client : eth0, 192.168.6.1
— Interface serveur DHCP : eth1, 192.168.7.1
— Serveur DHCP : 192.168.7.2

Il doit y avoir pour le serveur DHCP, une route qui accéde à l'objectif, ici il faut répondre à l'adresse 192.168.6.1, est-ce que le routeur sur lequel le relais fonctionne par défaut sur la passerelle peux accéder au serveur DHCP, si oui tout est ok.
Si ce n'est pas le cas, nous allons avoir besoin d'une extra route supplémentaire. Si le serveur DHCP veut accéder au client par le routeur fli4l, vous devez enregistrer dans config/base.txt : IP_ROUTE_x='192.168.6.0/24 192.168.7.1'

Pendant le fonctionnement, il y a parfois des messages d'avertissements au sujet de certains paquets ignorés, ne tenez pas compte de ces avertissements, cela a aucune incidance sur le fonctionnement normal.

Exemple :

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

1.1.5 Serveur TFTP

Un serveur TFTP peut être utilisé dans fli4l, pour la transmission de fichiers. Cela peut servir, par exemple, à un client pour récupérer des fichiers sur son portable par Internet.

OPT_TFTP Cette variable active le serveur TFTP interne du Dnsmasq. Le paramètre par défaut est 'no'.

TFTP_PATH Vous indiquez ici le répertoire du serveur TFTP dans lequel sera placé les fichiers, pour que les clients puissent les récupérer. Vous pouvez déposer les fichiers dans le chemin correspondant, à l'aide d'un programme adapté (par ex. scp).

1.1.6 YADIFA - Serveur DNS esclave

OPT_YADIFA Avec cette variable vous activez YADIFA, un serveur DNS esclave. Le paramètre par défaut est 'no'.

OPT_YADIFA_USE_DNSMASQ_ZONE_DELEGATION Si cette variable est activé, yadifa produira un script de démarrage qui génèrera automatiquement les entrées de toutes les zones esclaves correspondant au délégation de zone pour Dnsmasq. Ainsi, les zones d'esclaves sont directement interrogés par le Dnsmasq, en principe il ne sera pas nécessaire de configurer plusieurs fois YADIFA_LISTEN_x. Les réponces des requêtes de Dnsmasq sont transmises à yadifa qui écoute uniquement sur le port localhost :35353.

YADIFA_LISTEN_N Si vous avez activez `OPT_YADIFA`='yes', avec l'aide de la variable `YADIFA_LISTEN_N` vous indiquez le nombre d'adresses, si vous indiquez `YADIFA_LISTEN_1` vous devez spécifier une adresse IP du réseau local, sur laquelle YADIFA devra accepter les requêtes DNS. Un numéro de port est facultatif, si vous indiquez 192.168.1.1 :5353 le serveur DNS esclave YADIFA écoutera les requêtes DNS sur le port 5353. Assurez-vous que le Dnsmasq n'écoute pas sur toutes les interfaces (voir `DNS_BIND_INTERFACES`). A ce stade, seuls les adresses IP des interfaces existantes (Ethernet, Wlan, ...) peuvent être utilisé, sinon il y aura un message d'avertissement au démarrage du routeur. Il est également possible d'utiliser les alias, par ex. `IP_NET_1_IPADDR`

YADIFA_ALLOW_QUERY_N

YADIFA_ALLOW_QUERY_x Dans ces variables vous indiquer le nombre et les adresses IP ou les réseaux pour que YADIFA puis avoir une autorisation d'accès. YADIFA utilise les informations du filtrage de paquets de fli4l qui doit être configuré en conséquence, il faut aussi paramétrer les fichiers de configuration de YADIFA. En ajoutant le préfixe '!' à l'adresse, l'accès à l'adresse IP ou au réseau sera rejeté par YADIFA.

Le filtrage de paquets de fli4l est configuré pour YADIFA de sorte que tous les réseaux autosisés soient ajoutés dans chaque zone pour l'ensemble de la liste ipset (yadifa-allow-query). Une différenciation entre les zones pour le filtrage de paquets n'est pas possible. De plus toutes les adresses IP et de réseaux de la configuration globale dont l'accès est refusé seront ajoutées à cette liste. Il n'est donc pas possible d'étendre l'accès de chaque zone ultérieurement.

YADIFA_SLAVE_ZONE_N Dans cette variable vous indiquez le nombre de zone DNS pour YADIFA esclave.

YADIFA_SLAVE_ZONE_x Dans cette variable vous indiquez le nom de la zone DNS esclave.

OPT_YADIFA_SLAVE_ZONE_USE_DNSMASQ_ZONE_DELEGATION Dans cette variable vous activez (='yes') ou déactivez (='no') la délégation de zone pour la zone esclave du Dnsmasq.

YADIFA_SLAVE_ZONE_x_MASTER Dans cette variable vous indiquez l'adresse IP avec le numéro de port facultatif du serveur DNS maître.

YADIFA_SLAVE_ZONE_x_ALLOW_QUERY_N

YADIFA_SLAVE_ZONE_x_ALLOW_QUERY_x Dans ces variables vous indiquez le nombre et les adresses IP ou les réseaux, pour que YADIFA puis avoir une autorisation d'accès. En outre l'accès peut être limité à des zones DNS spécifiques. YADIFA utilise ces informations pour créer un fichier de configuration YADIFA.

En ajoutant le préfixe '!' à l'adresse, l'accès à l'adresse IP ou du réseau sera rejeté par YADIFA.

Table des figures

Liste des tableaux

Index