Logiciel

Dnsmasq : paramètres de configuration

Fichier de la distribution

```
# Configuration file for dnsmasq.
#
# Format is one option per line, legal options are the same
# as the long options legal on the command line. See
# "/usr/sbin/dnsmasq --help" or "man 8 dnsmasq" for details.

# Listen on this specific port instead of the standard DNS port
# (53). Setting this to zero completely disables DNS function,
# leaving only DHCP and/or TFTP.
#port=5353

# The following two options make you a better netizen, since they
# tell dnsmasq to filter out queries which the public DNS cannot
# answer, and which load the servers (especially the root servers)
# unnecessarily. If you have a dial-on-demand link they also stop
# these requests from bringing up the link unnecessarily.

# Never forward plain names (without a dot or domain part)
#domain-needed
# Never forward addresses in the non-routed address spaces.
#bogus-priv

# Uncomment these to enable DNSSEC validation and caching:
# (Requires dnsmasq to be built with DNSSEC option.)
#conf-file=%%PREFIX%%/share/dnsmasq/trust-anchors.conf
#dnssec

# Replies which are not DNSSEC signed may be legitimate, because the domain
# is unsigned, or may be forgeries. Setting this option tells dnsmasq to
# check that an unsigned reply is OK, by finding a secure proof that a DS
# record somewhere between the root and the domain does not exist.
# The cost of setting this is that even queries in unsigned domains will
need
# one or more extra DNS queries to verify.
#dnssec-check-unsigned

# Uncomment this to filter useless windows-originated DNS requests
# which can trigger dial-on-demand links needlessly.
# Note that (amongst other things) this blocks all SRV requests,
# so don't use it if you use eg Kerberos, SIP, XMMP or Google-talk.
# This option only affects forwarding, SRV records originating for
# dnsmasq (via srv-host= lines) are not suppressed by it.
```

```
#filterwin2k

# Change this line if you want dns to get its upstream servers from
# somewhere other that /etc/resolv.conf
#resolv-file=

# By  default,  dnsmasq  will  send queries to any of the upstream
# servers it knows about and tries to favour servers to are  known
# to  be  up.  Uncommenting this forces dnsmasq to try each query
# with  each  server  strictly  in  the  order  they   appear   in
# /etc/resolv.conf
#strict-order

# If you don't want dnsmasq to read /etc/resolv.conf or any other
# file, getting its servers from this file instead (see below), then
# uncomment this.
#no-resolv

# If you don't want dnsmasq to poll /etc/resolv.conf or other resolv
# files for changes and re-read them then uncomment this.
#no-poll

# Add other name servers here, with domain specs if they are for
# non-public domains.
#server=/localnet/192.168.0.1

# Example of routing PTR queries to nameservers: this will send all
# address->name queries for 192.168.3/24 to nameserver 10.1.2.3
#server=/3.168.192.in-addr.arpa/10.1.2.3

# Add local-only domains here, queries in these domains are answered
# from /etc/hosts or DHCP only.
#local=/localnet/

# Add domains which you want to force to an IP address here.
# The example below send any host in double-click.net to a local
# web-server.
#address=/double-click.net/127.0.0.1

# --address (and --server) work with IPv6 addresses too.
#address=/www.thekelleys.org.uk/fe80::20d:60ff:fe36:f83

# Add the IPs of all queries to yahoo.com, google.com, and their
# subdomains to the vpn and search ipsets:
#ipset=/yahoo.com/google.com/vpn,search

# You can control how dnsmasq talks to a server: this forces
# queries to 10.1.2.3 to be routed via eth1
# server=10.1.2.3@eth1
```

```
# and this sets the source (ie local) address used to talk to
# 10.1.2.3 to 192.168.1.1 port 55 (there must be an interface with that
# IP on the machine, obviously).
# server=10.1.2.3@192.168.1.1#55

# If you want dnsmasq to change uid and gid to something other
# than the default, edit the following lines.
#user=
#group=

# If you want dnsmasq to listen for DHCP and DNS requests only on
# specified interfaces (and the loopback) give the name of the
# interface (eg eth0) here.
# Repeat the line for more than one interface.
#interface=
# Or you can specify which interface _not_ to listen on
#except-interface=
# Or which to listen on by address (remember to include 127.0.0.1 if
# you use this.)
#listen-address=
# If you want dnsmasq to provide only DNS service on an interface,
# configure it as shown above, and then use the following line to
# disable DHCP and TFTP on it.
#no-dhcp-interface=

# On systems which support it, dnsmasq binds the wildcard address,
# even when it is listening on only some interfaces. It then discards
# requests that it shouldn't reply to. This has the advantage of
# working even when interfaces come and go and change address. If you
# want dnsmasq to really bind only the interfaces it is listening on,
# uncomment this option. About the only time you may need this is when
# running another nameserver on the same machine.
#bind-interfaces

# If you don't want dnsmasq to read /etc/hosts, uncomment the
# following line.
#no-hosts
# or if you want it to read another file, as well as /etc/hosts, use
# this.
#addn-hosts=/etc/banner_add_hosts

# Set this (and domain: see below) if you want to have a domain
# automatically added to simple names in a hosts-file.
#expand-hosts

# Set the domain for dnsmasq. this is optional, but if it is set, it
# does the following things.
# 1) Allows DHCP hosts to have fully qualified domain names, as long
#       as the domain part matches this setting.
# 2) Sets the "domain" DHCP option thereby potentially setting the
#     domain of all systems configured by DHCP
```

```
# 3) Provides the domain part for "expand-hosts"
#domain=thekelleys.org.uk

# Set a different domain for a particular subnet
#domain=wireless.thekelleys.org.uk,192.168.2.0/24

# Same idea, but range rather then subnet
#domain=reserved.thekelleys.org.uk,192.68.3.100,192.168.3.200

# Uncomment this to enable the integrated DHCP server, you need
# to supply the range of addresses available for lease and optionally
# a lease time. If you have more than one network, you will need to
# repeat this for each network on which you want to supply DHCP
# service.
#dhcp-range=192.168.0.50,192.168.0.150,12h

# This is an example of a DHCP range where the netmask is given. This
# is needed for networks we reach the dnsmasq DHCP server via a relay
# agent. If you don't know what a DHCP relay agent is, you probably
# don't need to worry about this.
#dhcp-range=192.168.0.50,192.168.0.150,255.255.255.0,12h

# This is an example of a DHCP range which sets a tag, so that
# some DHCP options may be set only for this network.
#dhcp-range=set:red,192.168.0.50,192.168.0.150

# Use this DHCP range only when the tag "green" is set.
#dhcp-range=tag:green,192.168.0.50,192.168.0.150,12h

# Specify a subnet which can't be used for dynamic address allocation,
# is available for hosts with matching --dhcp-host lines. Note that
# dhcp-host declarations will be ignored unless there is a dhcp-range
# of some type for the subnet in question.
# In this case the netmask is implied (it comes from the network
# configuration on the machine running dnsmasq) it is possible to give
# an explicit netmask instead.
#dhcp-range=192.168.0.0,static

# Enable DHCPv6. Note that the prefix-length does not need to be specified
# and defaults to 64 if missing/
#dhcp-range=1234::2, 1234::500, 64, 12h

# Do Router Advertisements, BUT NOT DHCP for this subnet.
#dhcp-range=1234::, ra-only

# Do Router Advertisements, BUT NOT DHCP for this subnet, also try and
# add names to the DNS for the IPv6 address of SLAAC-configured dual-stack
# hosts. Use the DHCPv4 lease to derive the name, network segment and
# MAC address and assume that the host will also have an
# IPv6 address calculated using the SLAAC algorithm.
```

```
#dhcp-range=1234::, ra-names

# Do Router Advertisements, BUT NOT DHCP for this subnet.
# Set the lifetime to 46 hours. (Note: minimum lifetime is 2 hours.)
#dhcp-range=1234::, ra-only, 48h

# Do DHCP and Router Advertisements for this subnet. Set the A bit in the RA
# so that clients can use SLAAC addresses as well as DHCP ones.
#dhcp-range=1234::2, 1234::500, slaac

# Do Router Advertisements and stateless DHCP for this subnet. Clients will
# not get addresses from DHCP, but they will get other configuration
information.
# They will use SLAAC for addresses.
#dhcp-range=1234::, ra-stateless

# Do stateless DHCP, SLAAC, and generate DNS names for SLAAC addresses
# from DHCPv4 leases.
#dhcp-range=1234::, ra-stateless, ra-names

# Do router advertisements for all subnets where we're doing DHCPv6
# Unless overridden by ra-stateless, ra-names, et al, the router
# advertisements will have the M and O bits set, so that the clients
# get addresses and configuration from DHCPv6, and the A bit reset, so the
# clients don't use SLAAC addresses.
#enable-ra

# Supply parameters for specified hosts using DHCP. There are lots
# of valid alternatives, so we will give examples of each. Note that
# IP addresses DO NOT have to be in the range given above, they just
# need to be on the same network. The order of the parameters in these
# do not matter, it's permissible to give name, address and MAC in any
# order.

# Always allocate the host with Ethernet address 11:22:33:44:55:66
# The IP address 192.168.0.60
#dhcp-host=11:22:33:44:55:66,192.168.0.60

# Always set the name of the host with hardware address
# 11:22:33:44:55:66 to be "fred"
#dhcp-host=11:22:33:44:55:66,fred

# Always give the host with Ethernet address 11:22:33:44:55:66
# the name fred and IP address 192.168.0.60 and lease time 45 minutes
#dhcp-host=11:22:33:44:55:66,fred,192.168.0.60,45m

# Give a host with Ethernet address 11:22:33:44:55:66 or
# 12:34:56:78:90:12 the IP address 192.168.0.60. Dnsmasq will assume
# that these two Ethernet interfaces will never be in use at the same
# time, and give the IP address to the second, even if it is already
# in use by the first. Useful for laptops with wired and wireless
```

```
# addresses.
#dhcp-host=11:22:33:44:55:66,12:34:56:78:90:12,192.168.0.60

# Give the machine which says its name is "bert" IP address
# 192.168.0.70 and an infinite lease
#dhcp-host=bert,192.168.0.70,infinite

# Always give the host with client identifier 01:02:02:04
# the IP address 192.168.0.60
#dhcp-host=id:01:02:02:04,192.168.0.60

# Always give the InfiniBand interface with hardware address
# 80:00:00:48:fe:80:00:00:00:00:00:f4:52:14:03:00:28:05:81 the
# ip address 192.168.0.61. The client id is derived from the prefix
# ff:00:00:00:00:00:02:00:00:02:c9:00 and the last 8 pairs of
# hex digits of the hardware address.
#dhcp-
host=id:ff:00:00:00:00:00:02:00:00:02:c9:00:f4:52:14:03:00:28:05:81,192.168.
0.61

# Always give the host with client identifier "marjorie"
# the IP address 192.168.0.60
#dhcp-host=id:marjorie,192.168.0.60

# Enable the address given for "judge" in /etc/hosts
# to be given to a machine presenting the name "judge" when
# it asks for a DHCP lease.
#dhcp-host=judge

# Never offer DHCP service to a machine whose Ethernet
# address is 11:22:33:44:55:66
#dhcp-host=11:22:33:44:55:66,ignore

# Ignore any client-id presented by the machine with Ethernet
# address 11:22:33:44:55:66. This is useful to prevent a machine
# being treated differently when running under different OS's or
# between PXE boot and OS boot.
#dhcp-host=11:22:33:44:55:66,id:*

# Send extra options which are tagged as "red" to
# the machine with Ethernet address 11:22:33:44:55:66
#dhcp-host=11:22:33:44:55:66,set:red

# Send extra options which are tagged as "red" to
# any machine with Ethernet address starting 11:22:33:
#dhcp-host=11:22:33:*:*:*,set:red

# Give a fixed IPv6 address and name to client with
# DUID 00:01:00:01:16:d2:83:fc:92:d4:19:e2:d8:b2
# Note the MAC addresses CANNOT be used to identify DHCPv6 clients.
```

```
# Note also that the [] around the IPv6 address are obligatory.
#dhcp-host=id:00:01:00:01:16:d2:83:fc:92:d4:19:e2:d8:b2, fred, [1234::5]

# Ignore any clients which are not specified in dhcp-host lines
# or /etc/ethers. Equivalent to ISC "deny unknown-clients".
# This relies on the special "known" tag which is set when
# a host is matched.
#dhcp-ignore=tag:!known

# Send extra options which are tagged as "red" to any machine whose
# DHCP vendorclass string includes the substring "Linux"
#dhcp-vendorclass=set:red,Linux

# Send extra options which are tagged as "red" to any machine one
# of whose DHCP userclass strings includes the substring "accounts"
#dhcp-userclass=set:red,accounts

# Send extra options which are tagged as "red" to any machine whose
# MAC address matches the pattern.
#dhcp-mac=set:red,00:60:8C:*:*:*

# If this line is uncommented, dnsmasq will read /etc/ethers and act
# on the ethernet-address/IP pairs found there just as if they had
# been given as --dhcp-host options. Useful if you keep
# MAC-address/host mappings there for other purposes.
#read-ethers

# Send options to hosts which ask for a DHCP lease.
# See RFC 2132 for details of available options.
# Common options can be given to dnsmasq by name:
# run "dnsmasq --help dhcp" to get a list.
# Note that all the common settings, such as netmask and
# broadcast address, DNS server and default route, are given
# sane defaults by dnsmasq. You very likely will not need
# any dhcp-options. If you use Windows clients and Samba, there
# are some options which are recommended, they are detailed at the
# end of this section.

# Override the default route supplied by dnsmasq, which assumes the
# router is the same machine as the one running dnsmasq.
#dhcp-option=3,1.2.3.4

# Do the same thing, but using the option name
#dhcp-option=option:router,1.2.3.4

# Override the default route supplied by dnsmasq and send no default
# route at all. Note that this only works for the options sent by
# default (1, 3, 6, 12, 28) the same line will send a zero-length option
# for all other option numbers.
#dhcp-option=3
```

```
# Set the NTP time server addresses to 192.168.0.4 and 10.10.0.5
#dhcp-option=option:ntp-server,192.168.0.4,10.10.0.5

# Send DHCPv6 option. Note [] around IPv6 addresses.
#dhcp-option=option6:dns-server,[1234::77],[1234::88]

# Send DHCPv6 option for namservers as the machine running
# dnsmasq and another.
#dhcp-option=option6:dns-server,[::],[1234::88]

# Ask client to poll for option changes every six hours. (RFC4242)
#dhcp-option=option6:information-refresh-time,6h

# Set option 58 client renewal time (T1). Defaults to half of the
# lease time if not specified. (RFC2132)
#dhcp-option=option:T1,1m

# Set option 59 rebinding time (T2). Defaults to 7/8 of the
# lease time if not specified. (RFC2132)
#dhcp-option=option:T2,2m

# Set the NTP time server address to be the same machine as
# is running dnsmasq
#dhcp-option=42,0.0.0.0

# Set the NIS domain name to "welly"
#dhcp-option=40,welly

# Set the default time-to-live to 50
#dhcp-option=23,50

# Set the "all subnets are local" flag
#dhcp-option=27,1

# Send the etherboot magic flag and then etherboot options (a string).
#dhcp-option=128,e4:45:74:68:00:00
#dhcp-option=129,NIC=eepro100

# Specify an option which will only be sent to the "red" network
# (see dhcp-range for the declaration of the "red" network)
# Note that the tag: part must precede the option: part.
#dhcp-option = tag:red, option:ntp-server, 192.168.1.1

# The following DHCP options set up dnsmasq in the same way as is specified
# for the ISC dhcpcd in
# http://www.samba.org/samba/ftp/docs/textdocs/DHCP-Server-Configuration.txt
# adapted for a typical dnsmasq installation where the host running
# dnsmasq is also the host running samba.
# you may want to uncomment some or all of them if you use
# Windows clients and Samba.
```

```
#dhcp-option=19,0            # option ip-forwarding off
#dhcp-option=44,0.0.0.0      # set netbios-over-TCP/IP nameserver(s) aka WINS
server(s)
#dhcp-option=45,0.0.0.0      # netbios datagram distribution server
#dhcp-option=46,8            # netbios node type

# Send an empty WPAD option. This may be REQUIRED to get windows 7 to
behave.
#dhcp-option=252,"\n"

# Send RFC-3397 DNS domain search DHCP option. WARNING: Your DHCP client
# probably doesn't support this......
#dhcp-option=option:domain-search,eng.apple.com,marketing.apple.com

# Send RFC-3442 classless static routes (note the netmask encoding)
#dhcp-option=121,192.168.1.0/24,1.2.3.4,10.0.0.0/8,5.6.7.8

# Send vendor-class specific options encapsulated in DHCP option 43.
# The meaning of the options is defined by the vendor-class so
# options are sent only when the client supplied vendor class
# matches the class given here. (A substring match is OK, so "MSFT"
# matches "MSFT" and "MSFT 5.0"). This example sets the
# mtftp address to 0.0.0.0 for PXEClients.
#dhcp-option=vendor:PXEClient,1,0.0.0.0

# Send microsoft-specific option to tell windows to release the DHCP lease
# when it shuts down. Note the "i" flag, to tell dnsmasq to send the
# value as a four-byte integer - that's what microsoft wants. See
#
http://technet2.microsoft.com/WindowsServer/en/library/a70f1bb7-d2d4-49f0-96
d6-4b7414ecfaae1033.mspx?mfr=true
#dhcp-option=vendor:MSFT,2,1i

# Send the Encapsulated-vendor-class ID needed by some configurations of
# Etherboot to allow is to recognise the DHCP server.
#dhcp-option=vendor:Etherboot,60,"Etherboot"

# Send options to PXELinux. Note that we need to send the options even
# though they don't appear in the parameter request list, so we need
# to use dhcp-option-force here.
# See http://syslinux.zytor.com/pxe.php#special for details.
# Magic number - needed before anything else is recognised
#dhcp-option-force=208,f1:00:74:7e
# Configuration file name
#dhcp-option-force=209,configs/common
# Path prefix
#dhcp-option-force=210,/tftpboot/pxelinux/files/
# Reboot time. (Note 'i' to send 32-bit value)
#dhcp-option-force=211,30i

# Set the boot filename for netboot/PXE. You will only need
```

```
# this if you want to boot machines over the network and you will need
# a TFTP server; either dnsmasq's built-in TFTP server or an
# external one. (See below for how to enable the TFTP server.)
#dhcp-boot=pxelinux.0

# The same as above, but use custom tftp-server instead machine running
dnsmasq
#dhcp-boot=pxelinux,server.name,192.168.1.100

# Boot for iPXE. The idea is to send two different
# filenames, the first loads iPXE, and the second tells iPXE what to
# load. The dhcp-match sets the ipxe tag for requests from iPXE.
#dhcp-boot=undionly.kpxe
#dhcp-match=set:ipxe,175 # iPXE sends a 175 option.
#dhcp-boot=tag:ipxe,http://boot.ipxe.org/demo/boot.php

# Encapsulated options for iPXE. All the options are
# encapsulated within option 175
#dhcp-option=encap:175, 1, 5b          # priority code
#dhcp-option=encap:175, 176, 1b        # no-proxydhcp
#dhcp-option=encap:175, 177, string    # bus-id
#dhcp-option=encap:175, 189, 1b        # BIOS drive code
#dhcp-option=encap:175, 190, user      # iSCSI username
#dhcp-option=encap:175, 191, pass      # iSCSI password

# Test for the architecture of a netboot client. PXE clients are
# supposed to send their architecture as option 93. (See RFC 4578)
#dhcp-match=peecees, option:client-arch, 0 #x86-32
#dhcp-match=itanics, option:client-arch, 2 #IA64
#dhcp-match=hammers, option:client-arch, 6 #x86-64
#dhcp-match=mactels, option:client-arch, 7 #EFI x86-64

# Do real PXE, rather than just booting a single file, this is an
# alternative to dhcp-boot.
#pxe-prompt="What system shall I netboot?"
# or with timeout before first available action is taken:
#pxe-prompt="Press F8 for menu.", 60

# Available boot services. for PXE.
#pxe-service=x86PC, "Boot from local disk"

# Loads <tftp-root>/pxelinux.0 from dnsmasq TFTP server.
#pxe-service=x86PC, "Install Linux", pxelinux

# Loads <tftp-root>/pxelinux.0 from TFTP server at 1.2.3.4.
# Beware this fails on old PXE ROMS.
#pxe-service=x86PC, "Install Linux", pxelinux, 1.2.3.4

# Use bootserver on network, found my multicast or broadcast.
#pxe-service=x86PC, "Install windows from RIS server", 1
```

```
# Use bootserver at a known IP address.
#pxe-service=x86PC, "Install windows from RIS server", 1, 1.2.3.4

# If you have multicast-FTP available,
# information for that can be passed in a similar way using options 1
# to 5. See page 19 of
# http://download.intel.com/design/archives/wfm/downloads/pxespec.pdf


# Enable dnsmasq's built-in TFTP server
#enable-tftp

# Set the root directory for files available via FTP.
#tftp-root=/var/ftpd

# Do not abort if the tftp-root is unavailable
#tftp-no-fail

# Make the TFTP server more secure: with this set, only files owned by
# the user dnsmasq is running as will be send over the net.
#tftp-secure

# This option stops dnsmasq from negotiating a larger blocksize for TFTP
# transfers. It will slow things down, but may rescue some broken TFTP
# clients.
#tftp-no-blocksize

# Set the boot file name only when the "red" tag is set.
#dhcp-boot=tag:red,pxelinux.red-net

# An example of dhcp-boot with an external TFTP server: the name and IP
# address of the server are given after the filename.
# Can fail with old PXE ROMS. Overridden by --pxe-service.
#dhcp-boot=/var/ftpd/pxelinux.0,boothost,192.168.0.3

# If there are multiple external tftp servers having a same name
# (using /etc/hosts) then that name can be specified as the
# tftp_servername (the third option to dhcp-boot) and in that
# case dnsmasq resolves this name and returns the resultant IP
# addresses in round robin fashion. This facility can be used to
# load balance the tftp load among a set of servers.
#dhcp-boot=/var/ftpd/pxelinux.0,boothost,tftp_server_name

# Set the limit on DHCP leases, the default is 150
#dhcp-lease-max=150

# The DHCP server needs somewhere on disk to keep its lease database.
# This defaults to a sane location, but if you want to change it, use
# the line below.
#dhcp-leasefile=/var/lib/misc/dnsmasq.leases
```

```
# Set the DHCP server to authoritative mode. In this mode it will barge in
# and take over the lease for any client which broadcasts on the network,
# whether it has a record of the lease or not. This avoids long timeouts
# when a machine wakes up on a new network. DO NOT enable this if there's
# the slightest chance that you might end up accidentally configuring a DHCP
# server for your campus/company accidentally. The ISC server uses
# the same option, and this URL provides more information:
# http://www.isc.org/files/auth.html
#dhcp-authoritative

# Run an executable when a DHCP lease is created or destroyed.
# The arguments sent to the script are "add" or "del",
# then the MAC address, the IP address and finally the hostname
# if there is one.
#dhcp-script=/bin/echo

# Set the cachesize here.
#cache-size=150

# If you want to disable negative caching, uncomment this.
#no-negcache

# Normally responses which come from /etc/hosts and the DHCP lease
# file have Time-To-Live set as zero, which conventionally means
# do not cache further. If you are happy to trade lower load on the
# server for potentially stale date, you can set a time-to-live (in
# seconds) here.
#local-ttl=

# If you want dnsmasq to detect attempts by Verisign to send queries
# to unregistered .com and .net hosts to its sitefinder service and
# have dnsmasq instead return the correct NXDOMAIN response, uncomment
# this line. You can add similar lines to do the same for other
# registries which have implemented wildcard A records.
#bogus-nxdomain=64.94.110.11

# If you want to fix up DNS results from upstream servers, use the
# alias option. This only works for IPv4.
# This alias makes a result of 1.2.3.4 appear as 5.6.7.8
#alias=1.2.3.4,5.6.7.8
# and this maps 1.2.3.x to 5.6.7.x
#alias=1.2.3.0,5.6.7.0,255.255.255.0
# and this maps 192.168.0.10->192.168.0.40 to 10.0.0.10->10.0.0.40
#alias=192.168.0.10-192.168.0.40,10.0.0.0,255.255.255.0

# Change these lines if you want dnsmasq to serve MX records.

# Return an MX record named "maildomain.com" with target
# servermachine.com and preference 50
```

```
#mx-host=maildomain.com,servermachine.com,50

# Set the default target for MX records created using the localmx option.
#mx-target=servermachine.com

# Return an MX record pointing to the mx-target for all local
# machines.
#localmx

# Return an MX record pointing to itself for all local machines.
#selfmx

# Change the following lines if you want dnsmasq to serve SRV
# records.  These are useful if you want to serve ldap requests for
# Active Directory and other windows-originated DNS requests.
# See RFC 2782.
# You may add multiple srv-host lines.
# The fields are <name>,<target>,<port>,<priority>,<weight>
# If the domain part if missing from the name (so that is just has the
# service and protocol sections) then the domain given by the domain=
# config option is used. (Note that expand-hosts does not need to be
# set for this to work.)

# A SRV record sending LDAP for the example.com domain to
# ldapserver.example.com port 389
#srv-host=_ldap._tcp.example.com,ldapserver.example.com,389

# A SRV record sending LDAP for the example.com domain to
# ldapserver.example.com port 389 (using domain=)
#domain=example.com
#srv-host=_ldap._tcp,ldapserver.example.com,389

# Two SRV records for LDAP, each with different priorities
#srv-host=_ldap._tcp.example.com,ldapserver.example.com,389,1
#srv-host=_ldap._tcp.example.com,ldapserver.example.com,389,2

# A SRV record indicating that there is no LDAP server for the domain
# example.com
#srv-host=_ldap._tcp.example.com

# The following line shows how to make dnsmasq serve an arbitrary PTR
# record. This is useful for DNS-SD. (Note that the
# domain-name expansion done for SRV records _does_not
# occur for PTR records.)
#ptr-record=_http._tcp.dns-sd-services,"New Employee Page._http._tcp.dns-sd-services"

# Change the following lines to enable dnsmasq to serve TXT records.
# These are used for things like SPF and zeroconf. (Note that the
# domain-name expansion done for SRV records _does_not
# occur for TXT records.)
```

```
#Example SPF.
#txt-record=example.com,"v=spf1 a -all"

#Example zeroconf
#txt-record=_http._tcp.example.com,name=value,paper=A4

# Provide an alias for a "local" DNS name. Note that this _only_ works
# for targets which are names from DHCP or /etc/hosts. Give host
# "bert" another name, bertrand
#cname=bertand,bert

# For debugging purposes, log each DNS query as it passes through
# dnsmasq.
#log-queries

# Log lots of extra information about DHCP transactions.
#log-dhcp

# Include another lot of configuration options.
#conf-file=/etc/dnsmasq.more.conf
#conf-dir=/etc/dnsmasq.d

# Include all the files in a directory except those ending in .bak
#conf-dir=/etc/dnsmasq.d,.bak

# Include all files in a directory which end in .conf
#conf-dir=/etc/dnsmasq.d/,*.conf
```

Format

- une option par ligne
- les options sont les mêmes que sur la ligne de commande.
- Voir dnsmasq –help ou "man 8 dnsmasq" pour plus de détails.

Réglages

port=5353
> Écoutez sur ce port spécifique au lieu du port DNS standard (53).
> Un réglage à zéro désactive complètement la fonction DNS, ne laissant que DHCP et / ou
> TFTP.

Les deux options suivantes font de vous un meilleur internaute, car elles indiquent à dnsmasq de
filtrer les requêtes auxquelles le DNS public ne peut pas répondre et qui chargent inutilement les
serveurs (en particulier les serveurs racine). Elles empêchent également ces demandes de faire

inutilement apparaître le lien.

domain-needed
>
> Ne transférez jamais de noms en clair (sans point ni partie de domaine)

bogus-priv
>
> Ne transférez jamais d'adresses dans les espaces d'adressage non routés.

Dé-commentez ces lignes pour activer la validation et la mise en cache DNSSEC: (Nécessite dnsmasq pour être construit avec l'option DNSSEC.)

#conf-file=PREFIX/share/dnsmasq/trust-anchors.conf
#dnssec

#dnssec-check-unsigned
>
> Les réponses qui ne sont pas signées DNSSEC peuvent être légitimes, car le domaine n'est pas signé, ou peuvent être des contrefaçons. Cette option indique à dnsmasq de vérifier qu'une réponse non signée est correcte, en trouvant une preuve sécurisée qu'un enregistrement DS quelque part entre la racine et le domaine n'existe pas. Le coût de cette configuration est que même les requêtes dans les domaines non signés auront besoin d'une ou plusieurs requêtes DNS supplémentaires pour vérifier.

Uncomment this to filter useless windows-originated DNS requests # which can trigger dial-on-demand links needlessly. # Note that (amongst other things) this blocks all SRV requests, # so don't use it if you use eg Kerberos, SIP, XMMP or Google-talk. # This option only affects forwarding, SRV records originating for # dnsmasq (via srv-host= lines) are not suppressed by it. #filterwin2k

Change this line if you want dns to get its upstream servers from # somewhere other that /etc/resolv.conf #resolv-file=

By default, dnsmasq will send queries to any of the upstream # servers it knows about and tries to favour servers to are known # to be up. Uncommenting this forces dnsmasq to try each query # with each server strictly in the order they appear in # /etc/resolv.conf #strict-order

If you don't want dnsmasq to read /etc/resolv.conf or any other # file, getting its servers from this file instead (see below), then # uncomment this. #no-resolv

If you don't want dnsmasq to poll /etc/resolv.conf or other resolv # files for changes and re-read them then uncomment this. #no-poll

server=/localnet/192.168.0.1
>
> Ajoutez d'autres serveurs de noms ici, avec les spécifications de domaine s'ils concernent des domaines non publics.
>
> Exemple de routage de requêtes PTR vers des serveurs de noms :
> server=/3.168.192.in-addr.arpa/10.1.2.3
>> cela enverra toutes les requêtes d'adresse→ nom pour 192.168.3/24 au serveur de noms 10.1.2.3

Add local-only domains here, queries in these domains are answered # from /etc/hosts or DHCP only. #local=/localnet/

Add domains which you want to force to an IP address here. # The example below send any host in double-click.net to a local # web-server. #address=/double-click.net/127.0.0.1

–address (and –server) work with IPv6 addresses too.
#address=/www.thekelleys.org.uk/fe80::20d:60ff:fe36:f83

Add the IPs of all queries to yahoo.com, google.com, and their # subdomains to the vpn and search ipsets: #ipset=/yahoo.com/google.com/vpn,search

You can control how dnsmasq talks to a server: this forces # queries to 10.1.2.3 to be routed via eth1 # server=10.1.2.3@eth1

and this sets the source (ie local) address used to talk to # 10.1.2.3 to 192.168.1.1 port 55 (there must be an interface with that # IP on the machine, obviously). # server=10.1.2.3@192.168.1.1#55

If you want dnsmasq to change uid and gid to something other # than the default, edit the following lines. #user= #group=

If you want dnsmasq to listen for DHCP and DNS requests only on # specified interfaces (and the loopback) give the name of the # interface (eg eth0) here. # Repeat the line for more than one interface. #interface= # Or you can specify which interface _not_ to listen on #except-interface= # Or which to listen on by address (remember to include 127.0.0.1 if # you use this.) #listen-address= # If you want dnsmasq to provide only DNS service on an interface, # configure it as shown above, and then use the following line to # disable DHCP and TFTP on it. #no-dhcp-interface=

On systems which support it, dnsmasq binds the wildcard address, # even when it is listening on only some interfaces. It then discards # requests that it shouldn't reply to. This has the advantage of # working even when interfaces come and go and change address. If you # want dnsmasq to really bind only the interfaces it is listening on, # uncomment this option. About the only time you may need this is when # running another nameserver on the same machine. #bind-interfaces

If you don't want dnsmasq to read /etc/hosts, uncomment the # following line. #no-hosts # or if you want it to read another file, as well as /etc/hosts, use # this. #addn-hosts=/etc/banner_add_hosts

Set this (and domain: see below) if you want to have a domain # automatically added to simple names in a hosts-file. #expand-hosts

Set the domain for dnsmasq. this is optional, but if it is set, it # does the following things. # 1) Allows DHCP hosts to have fully qualified domain names, as long # as the domain part matches this setting. # 2) Sets the "domain" DHCP option thereby potentially setting the # domain of all systems configured by DHCP # 3) Provides the domain part for "expand-hosts" #domain=thekelleys.org.uk

Set a different domain for a particular subnet #domain=wireless.thekelleys.org.uk,192.168.2.0/24

Same idea, but range rather then subnet
#domain=reserved.thekelleys.org.uk,192.68.3.100,192.168.3.200

Uncomment this to enable the integrated DHCP server, you need # to supply the range of addresses available for lease and optionally # a lease time. If you have more than one network, you will need to # repeat this for each network on which you want to supply DHCP # service. #dhcp-range=192.168.0.50,192.168.0.150,12h

This is an example of a DHCP range where the netmask is given. This # is needed for networks we reach the dnsmasq DHCP server via a relay # agent. If you don't know what a DHCP relay agent is, you probably # don't need to worry about this. #dhcp-range=192.168.0.50,192.168.0.150,255.255.255.0,12h

This is an example of a DHCP range which sets a tag, so that # some DHCP options may be set only for this network. #dhcp-range=set:red,192.168.0.50,192.168.0.150

Use this DHCP range only when the tag "green" is set. #dhcp-range=tag:green,192.168.0.50,192.168.0.150,12h

Specify a subnet which can't be used for dynamic address allocation, # is available for hosts with matching –dhcp-host lines. Note that # dhcp-host declarations will be ignored unless there is a dhcp-range # of some type for the subnet in question. # In this case the netmask is implied (it comes from the network # configuration on the machine running dnsmasq) it is possible to give # an explicit netmask instead. #dhcp-range=192.168.0.0,static

Enable DHCPv6. Note that the prefix-length does not need to be specified # and defaults to 64 if missing/ #dhcp-range=1234::2, 1234::500, 64, 12h

Do Router Advertisements, BUT NOT DHCP for this subnet. #dhcp-range=1234::, ra-only

Do Router Advertisements, BUT NOT DHCP for this subnet, also try and # add names to the DNS for the IPv6 address of SLAAC-configured dual-stack # hosts. Use the DHCPv4 lease to derive the name, network segment and # MAC address and assume that the host will also have an # IPv6 address calculated using the SLAAC algorithm. #dhcp-range=1234::, ra-names

Do Router Advertisements, BUT NOT DHCP for this subnet. # Set the lifetime to 46 hours. (Note: minimum lifetime is 2 hours.) #dhcp-range=1234::, ra-only, 48h

Do DHCP and Router Advertisements for this subnet. Set the A bit in the RA # so that clients can use SLAAC addresses as well as DHCP ones. #dhcp-range=1234::2, 1234::500, slaac

Do Router Advertisements and stateless DHCP for this subnet. Clients will # not get addresses from DHCP, but they will get other configuration information. # They will use SLAAC for addresses. #dhcp-range=1234::, ra-stateless

Do stateless DHCP, SLAAC, and generate DNS names for SLAAC addresses # from DHCPv4 leases. #dhcp-range=1234::, ra-stateless, ra-names

Do router advertisements for all subnets where we're doing DHCPv6 # Unless overridden by ra-stateless, ra-names, et al, the router # advertisements will have the M and O bits set, so that the clients # get addresses and configuration from DHCPv6, and the A bit reset, so the # clients don't use SLAAC addresses. #enable-ra

Supply parameters for specified hosts using DHCP. There are lots # of valid alternatives, so we will give examples of each. Note that # IP addresses DO NOT have to be in the range given above, they just # need to be on the same network. The order of the parameters in these # do not matter, it's permissible to give name, address and MAC in any # order.

Always allocate the host with Ethernet address 11:22:33:44:55:66 # The IP address 192.168.0.60 #dhcp-host=11:22:33:44:55:66,192.168.0.60

Always set the name of the host with hardware address # 11:22:33:44:55:66 to be "fred" #dhcp-host=11:22:33:44:55:66,fred

Always give the host with Ethernet address 11:22:33:44:55:66 # the name fred and IP address 192.168.0.60 and lease time 45 minutes #dhcp-host=11:22:33:44:55:66,fred,192.168.0.60,45m

Give a host with Ethernet address 11:22:33:44:55:66 or # 12:34:56:78:90:12 the IP address 192.168.0.60. Dnsmasq will assume # that these two Ethernet interfaces will never be in use at the same # time, and give the IP address to the second, even if it is already # in use by the first. Useful for laptops with wired and wireless # addresses. #dhcp-host=11:22:33:44:55:66,12:34:56:78:90:12,192.168.0.60

Give the machine which says its name is "bert" IP address # 192.168.0.70 and an infinite lease #dhcp-host=bert,192.168.0.70,infinite

Always give the host with client identifier 01:02:02:04 # the IP address 192.168.0.60 #dhcp-host=id:01:02:02:04,192.168.0.60

Always give the InfiniBand interface with hardware address # 80:00:00:48:fe:80:00:00:00:00:00:00:f4:52:14:03:00:28:05:81 the # ip address 192.168.0.61. The client id is derived from the prefix # ff:00:00:00:00:00:02:00:00:02:c9:00 and the last 8 pairs of # hex digits of the hardware address. #dhcp-host=id:ff:00:00:00:00:00:02:00:00:02:c9:00:f4:52:14:03:00:28:05:81,192.168.0.61

Always give the host with client identifier "marjorie" # the IP address 192.168.0.60 #dhcp-host=id:marjorie,192.168.0.60

Enable the address given for "judge" in /etc/hosts # to be given to a machine presenting the name "judge" when # it asks for a DHCP lease. #dhcp-host=judge

Never offer DHCP service to a machine whose Ethernet # address is 11:22:33:44:55:66 #dhcp-host=11:22:33:44:55:66,ignore

Ignore any client-id presented by the machine with Ethernet # address 11:22:33:44:55:66. This is useful to prevent a machine # being treated differently when running under different OS's or # between PXE boot and OS boot. #dhcp-host=11:22:33:44:55:66,id:*

Send extra options which are tagged as "red" to # the machine with Ethernet address 11:22:33:44:55:66 #dhcp-host=11:22:33:44:55:66,set:red

Send extra options which are tagged as "red" to # any machine with Ethernet address starting 11:22:33: #dhcp-host=11:22:33:*:*:*,set:red

Give a fixed IPv6 address and name to client with # DUID 00:01:00:01:16:d2:83:fc:92:d4:19:e2:d8:b2 # Note the MAC addresses CANNOT be used to identify DHCPv6 clients. # Note also that the [] around the IPv6 address are obligatory. #dhcp-host=id:00:01:00:01:16:d2:83:fc:92:d4:19:e2:d8:b2, fred, [1234::5]

Ignore any clients which are not specified in dhcp-host lines # or /etc/ethers. Equivalent to ISC "deny unknown-clients". # This relies on the special "known" tag which is set when # a host is matched. #dhcp-ignore=tag:!known

Send extra options which are tagged as "red" to any machine whose # DHCP vendorclass string includes the substring "Linux" #dhcp-vendorclass=set:red,Linux

Send extra options which are tagged as "red" to any machine one # of whose DHCP userclass strings includes the substring "accounts" #dhcp-userclass=set:red,accounts

Send extra options which are tagged as "red" to any machine whose # MAC address matches the pattern. #dhcp-mac=set:red,00:60:8C:*:*:*

If this line is uncommented, dnsmasq will read /etc/ethers and act # on the ethernet-address/IP pairs found there just as if they had # been given as –dhcp-host options. Useful if you keep # MAC-address/host mappings there for other purposes. #read-ethers

Send options to hosts which ask for a DHCP lease. # See RFC 2132 for details of available options. # Common options can be given to dnsmasq by name: # run "dnsmasq –help dhcp" to get a list. # Note that all the common settings, such as netmask and # broadcast address, DNS server and default route, are given # sane defaults by dnsmasq. You very likely will not need # any dhcp-options. If you use Windows clients and Samba, there # are some options which are recommended, they are detailed at the # end of this section.

Override the default route supplied by dnsmasq, which assumes the # router is the same machine as the one running dnsmasq. #dhcp-option=3,1.2.3.4

Do the same thing, but using the option name #dhcp-option=option:router,1.2.3.4

Override the default route supplied by dnsmasq and send no default # route at all. Note that this only works for the options sent by # default (1, 3, 6, 12, 28) the same line will send a zero-length option # for all other option numbers. #dhcp-option=3

Set the NTP time server addresses to 192.168.0.4 and 10.10.0.5 #dhcp-option=option:ntp-server,192.168.0.4,10.10.0.5

Send DHCPv6 option. Note [] around IPv6 addresses. #dhcp-option=option6:dns-server,[1234::77],[1234::88]

Send DHCPv6 option for namservers as the machine running # dnsmasq and another. #dhcp-option=option6:dns-server,[::],[1234::88]

Ask client to poll for option changes every six hours. (RFC4242) #dhcp-option=option6:information-refresh-time,6h

Set option 58 client renewal time (T1). Defaults to half of the # lease time if not specified. (RFC2132) #dhcp-option=option:T1,1m

Set option 59 rebinding time (T2). Defaults to 7/8 of the # lease time if not specified. (RFC2132) #dhcp-option=option:T2,2m

Set the NTP time server address to be the same machine as # is running dnsmasq #dhcp-option=42,0.0.0.0

Set the NIS domain name to "welly" #dhcp-option=40,welly

Set the default time-to-live to 50 #dhcp-option=23,50

Set the "all subnets are local" flag #dhcp-option=27,1

Send the etherboot magic flag and then etherboot options (a string). #dhcp-option=128,e4:45:74:68:00:00 #dhcp-option=129,NIC=eepro100

Specify an option which will only be sent to the "red" network # (see dhcp-range for the declaration of the "red" network) # Note that the tag: part must precede the option: part. #dhcp-option = tag:red, option:ntp-server, 192.168.1.1

The following DHCP options set up dnsmasq in the same way as is specified # for the ISC dhcpcd in # http://www.samba.org/samba/ftp/docs/textdocs/DHCP-Server-Configuration.txt # adapted for a typical dnsmasq installation where the host running # dnsmasq is also the host running samba. # you may want to uncomment some or all of them if you use # Windows clients and Samba. #dhcp-option=19,0 # option ip-forwarding off #dhcp-option=44,0.0.0.0 # set netbios-over-TCP/IP nameserver(s) aka WINS server(s) #dhcp-option=45,0.0.0.0 # netbios datagram distribution server #dhcp-option=46,8 # netbios node type

Send an empty WPAD option. This may be REQUIRED to get windows 7 to behave. #dhcp-option=252,"\n"

Send RFC-3397 DNS domain search DHCP option. WARNING: Your DHCP client # probably doesn't support this...... #dhcp-option=option:domain-search,eng.apple.com,marketing.apple.com

Send RFC-3442 classless static routes (note the netmask encoding) #dhcp-option=121,192.168.1.0/24,1.2.3.4,10.0.0.0/8,5.6.7.8

Send vendor-class specific options encapsulated in DHCP option 43. # The meaning of the options is defined by the vendor-class so # options are sent only when the client supplied vendor class # matches the class given here. (A substring match is OK, so "MSFT" # matches "MSFT" and "MSFT 5.0"). This example sets the # mtftp address to 0.0.0.0 for PXEClients. #dhcp-option=vendor:PXEClient,1,0.0.0.0

Send microsoft-specific option to tell windows to release the DHCP lease # when it shuts down. Note the "i" flag, to tell dnsmasq to send the # value as a four-byte integer - that's what microsoft wants. See # http://technet2.microsoft.com/WindowsServer/en/library/a70f1bb7-d2d4-49f0-96d6-4b7414ecfaae1033.mspx?mfr=true #dhcp-option=vendor:MSFT,2,1i

Send the Encapsulated-vendor-class ID needed by some configurations of # Etherboot to allow is to recognise the DHCP server. #dhcp-option=vendor:Etherboot,60,"Etherboot"

Send options to PXELinux. Note that we need to send the options even # though they don't appear in the parameter request list, so we need # to use dhcp-option-force here. # See http://syslinux.zytor.com/pxe.php#special for details. # Magic number - needed before anything else is recognised #dhcp-option-force=208,f1:00:74:7e # Configuration file name #dhcp-option-force=209,configs/common # Path prefix #dhcp-option-force=210,/tftpboot/pxelinux/files/ # Reboot time. (Note 'i' to send 32-bit value) #dhcp-option-force=211,30i

Set the boot filename for netboot/PXE. You will only need # this if you want to boot machines over the network and you will need # a TFTP server; either dnsmasq's built-in TFTP server or an # external one. (See below for how to enable the TFTP server.) #dhcp-boot=pxelinux.0

The same as above, but use custom tftp-server instead machine running dnsmasq #dhcp-boot=pxelinux,server.name,192.168.1.100

Boot for iPXE. The idea is to send two different # filenames, the first loads iPXE, and the second tells iPXE what to # load. The dhcp-match sets the ipxe tag for requests from iPXE. #dhcp-boot=undionly.kpxe #dhcp-match=set:ipxe,175 # iPXE sends a 175 option. #dhcp-boot=tag:ipxe,http://boot.ipxe.org/demo/boot.php

Encapsulated options for iPXE. All the options are # encapsulated within option 175 #dhcp-option=encap:175, 1, 5b # priority code #dhcp-option=encap:175, 176, 1b # no-proxydhcp #dhcp-option=encap:175, 177, string # bus-id #dhcp-option=encap:175, 189, 1b # BIOS drive code #dhcp-option=encap:175, 190, user # iSCSI username #dhcp-option=encap:175, 191, pass # iSCSI password

Test for the architecture of a netboot client. PXE clients are # supposed to send their architecture as option 93. (See RFC 4578) #dhcp-match=peecees, option:client-arch, 0 #x86-32 #dhcp-match=itanics, option:client-arch, 2 #IA64 #dhcp-match=hammers, option:client-arch, 6 #x86-64 #dhcp-match=mactels, option:client-arch, 7 #EFI x86-64

Do real PXE, rather than just booting a single file, this is an # alternative to dhcp-boot. #pxe-prompt="What system shall I netboot?" # or with timeout before first available action is taken: #pxe-prompt="Press F8 for menu.", 60

Available boot services. for PXE. #pxe-service=x86PC, "Boot from local disk"

Loads <tftp-root>/pxelinux.0 from dnsmasq TFTP server. #pxe-service=x86PC, "Install Linux", pxelinux

Loads <tftp-root>/pxelinux.0 from TFTP server at 1.2.3.4. # Beware this fails on old PXE ROMS. #pxe-service=x86PC, "Install Linux", pxelinux, 1.2.3.4

Use bootserver on network, found my multicast or broadcast. #pxe-service=x86PC, "Install windows from RIS server", 1

Use bootserver at a known IP address. #pxe-service=x86PC, "Install windows from RIS server", 1, 1.2.3.4

If you have multicast-FTP available, # information for that can be passed in a similar way using options 1 # to 5. See page 19 of # http://download.intel.com/design/archives/wfm/downloads/pxespec.pdf

Enable dnsmasq's built-in TFTP server #enable-tftp

Set the root directory for files available via FTP. #tftp-root=/var/ftpd

Do not abort if the tftp-root is unavailable #tftp-no-fail

Make the TFTP server more secure: with this set, only files owned by # the user dnsmasq is running as will be send over the net. #tftp-secure

This option stops dnsmasq from negotiating a larger blocksize for TFTP # transfers. It will slow things down, but may rescue some broken TFTP # clients. #tftp-no-blocksize

Set the boot file name only when the "red" tag is set. #dhcp-boot=tag:red,pxelinux.red-net

An example of dhcp-boot with an external TFTP server: the name and IP # address of the server are given after the filename. # Can fail with old PXE ROMS. Overridden by –pxe-service. #dhcp-boot=/var/ftpd/pxelinux.0,boothost,192.168.0.3

If there are multiple external tftp servers having a same name # (using /etc/hosts) then that name can be specified as the # tftp_servername (the third option to dhcp-boot) and in that # case dnsmasq resolves this name and returns the resultant IP # addresses in round robin fashion. This facility can be used to # load balance the tftp load among a set of servers. #dhcp-boot=/var/ftpd/pxelinux.0,boothost,tftp_server_name

Set the limit on DHCP leases, the default is 150 #dhcp-lease-max=150

The DHCP server needs somewhere on disk to keep its lease database. # This defaults to a sane location, but if you want to change it, use # the line below. #dhcp-leasefile=/var/lib/misc/dnsmasq.leases

Set the DHCP server to authoritative mode. In this mode it will barge in # and take over the lease for any client which broadcasts on the network, # whether it has a record of the lease or not. This avoids long timeouts # when a machine wakes up on a new network. DO NOT enable this if there's # the slightest chance that you might end up accidentally configuring a DHCP # server for your campus/company accidentally. The ISC server uses # the same option, and this URL provides more information: # http://www.isc.org/files/auth.html #dhcp-authoritative

Run an executable when a DHCP lease is created or destroyed. # The arguments sent to the script are "add" or "del", # then the MAC address, the IP address and finally the hostname # if there is one. #dhcp-script=/bin/echo

Set the cachesize here. #cache-size=150

If you want to disable negative caching, uncomment this. #no-negcache

Normally responses which come from /etc/hosts and the DHCP lease # file have Time-To-Live set as zero, which conventionally means # do not cache further. If you are happy to trade lower load on the # server for potentially stale date, you can set a time-to-live (in # seconds) here. #local-ttl=

If you want dnsmasq to detect attempts by Verisign to send queries # to unregistered .com and .net hosts to its sitefinder service and # have dnsmasq instead return the correct NXDOMAIN response, uncomment # this line. You can add similar lines to do the same for other # registries which have implemented wildcard A records. #bogus-nxdomain=64.94.110.11

If you want to fix up DNS results from upstream servers, use the # alias option. This only works for IPv4. # This alias makes a result of 1.2.3.4 appear as 5.6.7.8 #alias=1.2.3.4,5.6.7.8 # and this maps 1.2.3.x to 5.6.7.x #alias=1.2.3.0,5.6.7.0,255.255.255.0 # and this maps 192.168.0.10→192.168.0.40 to 10.0.0.10→10.0.0.40 #alias=192.168.0.10-192.168.0.40,10.0.0.0,255.255.255.0

Change these lines if you want dnsmasq to serve MX records.

Return an MX record named "maildomain.com" with target # servermachine.com and preference 50 #mx-host=maildomain.com,servermachine.com,50

Set the default target for MX records created using the localmx option. #mx-target=servermachine.com

Return an MX record pointing to the mx-target for all local # machines. #localmx

Return an MX record pointing to itself for all local machines. #selfmx

Change the following lines if you want dnsmasq to serve SRV # records. These are useful if you want to serve ldap requests for # Active Directory and other windows-originated DNS requests. # See RFC 2782. # You may add multiple srv-host lines. # The fields are <name>,<target>,<port>,<priority>,<weight> # If the domain part if missing from the name (so that is just has the # service and protocol sections) then the domain given by the domain= # config option is used. (Note that expand-hosts does not need to be # set for this to work.)

A SRV record sending LDAP for the example.com domain to # ldapserver.example.com port 389 #srv-host=_ldap._tcp.example.com,ldapserver.example.com,389

A SRV record sending LDAP for the example.com domain to # ldapserver.example.com port 389 (using domain=) #domain=example.com #srv-host=_ldap._tcp,ldapserver.example.com,389

Two SRV records for LDAP, each with different priorities #srv-host=_ldap._tcp.example.com,ldapserver.example.com,389,1 #srv-host=_ldap._tcp.example.com,ldapserver.example.com,389,2

A SRV record indicating that there is no LDAP server for the domain # example.com #srv-host=_ldap._tcp.example.com

The following line shows how to make dnsmasq serve an arbitrary PTR # record. This is useful for DNS-SD. (Note that the # domain-name expansion done for SRV records _does_not # occur for PTR records.) #ptr-record=_http._tcp.dns-sd-services,"New Employee Page._http._tcp.dns-sd-services"

Change the following lines to enable dnsmasq to serve TXT records. # These are used for things like SPF and zeroconf. (Note that the # domain-name expansion done for SRV records _does_not # occur for TXT records.)

#Example SPF. #txt-record=example.com,"v=spf1 a -all"

#Example zeroconf #txt-record=_http._tcp.example.com,name=value,paper=A4

Provide an alias for a "local" DNS name. Note that this _only_ works # for targets which are names from DHCP or /etc/hosts. Give host # "bert" another name, bertrand #cname=bertand,bert

For debugging purposes, log each DNS query as it passes through # dnsmasq. #log-queries

Log lots of extra information about DHCP transactions. #log-dhcp

Include another lot of configuration options. #conf-file=/etc/dnsmasq.more.conf #conf-dir=/etc/dnsmasq.d

Include all the files in a directory except those ending in .bak #conf-dir=/etc/dnsmasq.d,.bak

Include all files in a directory which end in .conf #conf-dir=/etc/dnsmasq.d/,*.conf

Voir aussi

- **(fr)** http://

Basé sur « Article » par Auteur.

From:
http://doc.nfrappe.fr/ - **Documentation du Dr Nicolas Frappé**

Permanent link:
http://doc.nfrappe.fr/doku.php?id=logiciel:internet:dnsmasq:ubuntu18.04:config

Last update: **2022/11/08 19:27**