

DNS配置

dns配置位于 `/etc/config/dhcp` 并控制设备上的DNS (Domain Name System)和DHCP服务器选项 (DHCP和DNS (Domain Name System)服务都使用*dnsmasq*实现)。

在默认配置中，此文件包含一个公共部分，用于指定DNS (Domain Name System)和守护程序相关选项以及一个或多个DHCP池，以在网络接口上定义DHCP服务。

第

dhcp 配置文件的可能部分类型定义如下。并非所有类型都可能出现在文件中，并且大多数类型只能用于特殊配置。在常用的是常用选项，则DHCP地址池和静态租赁。

常用选项

配置部分类型 *dnsmasq* 确定与所有接口上的*dnsmasq*和DHCP选项的整体操作相关的值和选项。下表列出了所有可用的选项，它们的默认值以及相应的*dnsmasq*命令行选项。有关详细信息，请参阅*dnsmasq*手册页 (<http://www.thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html>)。

这些是常用选项的默认设置：

```
config 'dnsmasq'
    期权域名1
    选项boguspriv 1
    选项filterwin2k 0
    选项localise_queries 1
    选项rebind_protection 1
    选项rebind_localhost 0
    选项本地 '/ lan /'
    选项域 'lan'
    选项expandhosts 1
    选项nonegcache 0
    选项权威1
    选项readethers 1
    option leasefile '/tmp/dhcp.leases'
    选项resolvfile '/tmp/resolv.conf.auto'
```

- 选项 `local` 和 `domain` 支持的*dnsmasq*服务于项目 `/etc/hosts`，好像他们是进入以及DHCP客户端的名兰 DNS (Domain Name System)域名。
- 选项 `domainneeded`，`boguspriv`，`localise_queries`，并 `expandhosts` 确保这些本地主机名 (和反向查找) 永远不会转发到上游请求DNS (Domain Name System)服务器。
- 选项 `authoritative` 使路由器成为该网络上唯一的DHCP服务器; 客户以这种方式获得更多的IP租约。

- 选项 `leasefile` 将租约存储在文件中，以便如果重新启动 `dnsmasq`，则可以重新拾取租约。
- 选项 `resolvfile` 告诉 `dnsmasq` 使用此文件查找上游名称服务器；它由 WAN DHCP 客户端或 PPP 客户端创建。
- 选项“`enable_tftp`”和“`tftp_root`”打开 TFTP 服务器，并从 `tftp_root` 提供文件。您可能需要在客户端上设置服务器的 IP。在客户端，通过设置“`serverip`”来更改它（例如“`setenv serverip 192.168.1.10`”）。

所有选项

名称	类型	默认	选项	描述
<code>add_local_domain</code>	布尔	1		将 <code>resolv.conf</code> 中的本地域添加为搜索指令。
<code>add_local_hostname</code>	布尔	1		仅在 DHCP 服务的 LAN (Local Area Network) 上为此路由器添加 A, AAAA 和 PTR 记录。  增强功能可用于 Trunk 上的选项 <code>add_local_fqdn</code>
<code>add_local_fqdn</code>	整数	1		仅在 DHCP 服务的 LAN (Local Area Network) 上为此路由器添加 A, AAAA 和 PTR 记录。0 - 禁用。1 - 主地址上的主机名。2 - 所有地址上的主机名。3 - 所有地址上的 FDQN。4 - <code>iface.host.domain</code> 所有地址。  <code>add_local_fqdn</code> 在中继，但不是 17.01.0
<code>add_wan_fqdn</code>	整数	0		标签 WAN 接口， <code>add_local_fqdn</code> 而不是您的 ISP 分配的默认值，这可能是模糊的。WAN 从 <code>config dhcp</code> 具有 <code>option ignore 1</code> 集合的部分推断出来，因此不需要在中继线上命名为 WAN  <code>add_wan_fqdn</code> ，而不是 17.01.0
<code>addnhosts</code>	文件路径列表	(没有)	-H	读取的其他主机文件用于提供 DNS (Domain Name System) 响应
<code>authoritative</code>	布尔	1	-K	强制 <code>dnsmasq</code> 进入权威模式。这样可以加快 DHCP 的租用速度。用于网络上唯一的服务器
<code>bogusnxdomain</code>	IP 地址	(没有)	-B	转换为 NXDOMAIN 响应的 IP 地址（以抵消从不返回 NXDOMAIN 的“有用的”上游 DNS (Domain Name

	列表				<u>System</u>)服务器)。
boguspriv	布尔	0	-b		拒绝反向查找到私有IP范围，其中不存在相应的条目 /etc/hosts
cachelocal	布尔	1			设置时 0，使用 dns 本地的每个网络接口的地址 /etc/resolv.conf。通常只使用环回地址，所有查询都通过 <i>dnsmasq</i> 。
cache-size	整数	150	-c		尺寸的 <i>dnsmasq</i> 查询缓存。
dbus	布尔	0	-1		启用 <i>dnsmasq</i> 的DBus消息传递。 <i>OpenWRT</i> 上  的 <i>dnsmasq</i> 的标准版本不包括DBus支持。
dhcp_boot	串	(没有)		--dhcp启动	指定BOOTP选项，在大多数情况下只是文件名。你也可以使用“ file name, tftp server name, tftp ip address “
dhcp-hostsfile	文件路径	(没有)		--dhcp-hosts文件	使用每个主机DHCP选项指定一个外部文件
dhcp-lease-max	整数	150	-X		DHCP租约的最大数量
dns-forward-max	整数	150	-0 (零)		最大并发连接数
domain	域名	(没有)	-s		<u>DNS (Domain Name System)</u> 域发送给DHCP客户端
domain-needed	布尔	1	-D		告诉 <i>dnsmasq</i> 不要向上游名称服务器转发没有点或域部件的纯名称查询。如果从/ etc / hosts或DHCP不知道该名称，则返回“未找到”答案
dnssec	布尔	0		--dnsssec	验证 <u>DNS (Domain Name System)</u> 回复并缓存DNSSEC数据。  需要 <i>dnsmasq-full</i> 包。
dnssec-check-unsigned	布尔	0			检查未签名回复的区域以确保在这些区域中允许未签名的回复。这样可以防止攻击者伪造签名的 <u>DNS (Domain Name System)</u> 区域的未签名回复，但是较慢，并且要求 <i>dnsmasq</i> 上游的

			<pre>--dn ssec 检 查, 无符 号</pre>	<p>名称服务器具有DNSSEC能力。</p> <p>⚠需要<i>dnsmasq-full</i>包。</p> <p>⚠注意：如果在没有硬件时钟的设备上使用此选项，由于系统时间不正确，<i>dns</i>解析可能会在设备重启后中断。</p>
ednspacket_max	整数	1280	-P	指定DNS (Domain Name System)转发器支持的最大的EDNS.0 UDP数据包
enable_tftp	布尔	0	<pre>--en able -TFT P</pre>	启用内置TFTP服务器
expandhosts	布尔	1	-E	将本地域部分添加到找到的名称 /etc/hosts
filterwin2k	布尔	0	-f	不要转发公共名称服务器无法应答的请求
fqdn	布尔	0	<pre>--dh cp-F QDN</pre>	不解决不合格的本地主机名。需要domain 设置
interface	接口名称列表	(所有接口)	-i	要监听的接口列表。如果未指定， <i>dnsmasq</i> 将侦听除列出的所有接口之外的所有接口 <i>notinterface</i> 。请注意， <i>dnsmasq</i> 默认监听环回。
leasefile	文件路径	(没有)	-l (ELL)	在此文件中存储DHCP租约
local	串	(没有)	-S	查找此域的DNS (Domain Name System)条目 /etc/hosts。这与 <i>server</i> 条目遵循相同的语法，请参见手册页。
localise_queries	布尔	0	-y	如果多个地址分配给主机名，请选择IP地址以匹配传入接口 /etc/hosts。⚠请注意此选项的拼写。
localservice	布尔	1		接受DNS (Domain Name System)只能从主机地址为本地子网中的查询，

				--local 服务	即对于该服务器上存在的接口的子网。
logqueries	布尔	0		-q	记录DNS (Domain Name System)查询的结果，转储缓存在SIGUSR1上
nodaemon	布尔	0		-d	不要守护进程dnsmasq
nohosts	布尔	0		-h	不要从中读取DNS (Domain Name System)名称 /etc/hosts
nonegcache	布尔	0		-N	禁用缓存消息“否”这样的域“响应
noresolv	布尔	0		-R	不要从上游服务器读取 /etc/resolv.conf
notinterface	接口名称列表	(没有)		-I (眼)	接口dnsmasq不应该监听。
nonwildcard	布尔	0		-z	仅绑定配置的接口地址，而不是通配符地址。
port	端口号	53		-p	DNS (Domain Name System)查询的侦听端口，如果设置为禁用DNS (Domain Name System)服务器功能 0
queryport	整数	(没有)		-Q	使用固定端口进行出站DNS (Domain Name System)查询
readethers	布尔	0		-Z	读取静态租约条目 /etc/ethers，重新读取SIGHUP
rebind_protection	布尔	1		--st op-D NS- 重新 绑定	通过丢弃上游RFC1918响应启用DNS (Domain Name System)重新绑定攻击防护
rebind_localhost	布尔	0			允许基于DNS (Domain Name System)的黑名单服务所需的上游127.0.0.0/8响应仅在启用重新绑定保护时生效

			<code>--rebind</code> -本地主机-O K	
<code>rebind_domain</code>	域名列表	(没有)	<code>--rebind域-O K</code>	允许RFC1918响应的域列表仅在启用重新绑定保护时生效
<code>resolvfile</code>	文件路径	<code>/etc/resolv.conf</code>	<code>-r</code>	指定一个替代的resolv文件
<code>server</code>	字符串列表	(没有)	<code>-S</code>	将请求转发到的DNS (Domain Name System)服务器列表。有关语法详细信息，请参阅 <i>dnsmasq</i> 手册页。
<code>strictorder</code>	布尔	<code>0</code>	<code>-o</code>	服从DNS (Domain Name System)服务器的顺序 <code>/etc/resolv.conf</code>
<code>tftp_root</code>	目录路径	(没有)	<code>--tftp根</code>	指定TFTP根目录

使用简单的dnsmasq.conf

可以将传统 `/etc/dnsmasq.conf` 配置文件与其中的选项进行混合 `/etc/config/dhcp` 。

`dnsmasq.conf` 默认情况下 该文件不存在，但如果存在，将在启动时由*dnsmasq*进行处理。请注意，在选择 `/etc/config/dhcp` 采取precedence了 `dnsmasq.conf` ，因为它们被翻译为命令行参数。

您可以 `dnsmasq` 对每个动作执行脚本：

```
DHCP-脚本= / sbin目录/ action.sh
```

DNS端口

DNS (Domain Name System)需要在防火墙上打开TCP和UDP端口53。请参阅<http://wiki.openwrt.org/doc/recipes/guest-wlan> (<http://wiki.openwrt.org/doc/recipes/guest-wlan>) 和<http://www.thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html> (<http://www.thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html>) (即“-dhcp-alternate-port”) 了解更多信息。

例子

自定义域

定义自定义域名和相应的PTR记录 - 将IP地址分配给 192.168.1.140 域名 typhoon 并构建适当的反向记录 140.1.168.192.in-addr.arpa。它的工作原理就像一个条目， /etc/hosts 但更灵活和集成。

⚠ 请注意，此功能目前仅适用于IPv4地址，并且该功能在8.09.2之前的版本中不存在。

⚠ 请注意，目前无法正确生成反向记录。(阻隔断路器14.07-RC2)

```
配置'域'  
    选项'name' 'typhoon'  
    选项'ip' '192.168.1.140'
```

另一个例子：重定向www.facebook.com (<http://www.facebook.com>)

```
配置'域'  
    选项'name' 'www.facebook.com'  
    选项'ip' '1.2.3.4'  
    #www.bookbook.com的请求将以1.2.3.4结束
```

SIP的SRV RR

要定义SIP over UDP的SRV记录，主机pbx.mydomain.com上的默认端口为5060，类为0，权值为10，可以使用：

```
config'srvhost'  
    选项'srv' '_sip._udp.mydomain.com'  
    选项目标'pbx.mydomain.com'  
    选项端口5060  
    选项类0  
    选项权重10
```

CNAME RR

规范名称记录指定域名是另一个域(“规范”域)的别名。要指定Web服务器也兼作FTP (File Transfer Protocol)服务器，可以使用：

```
config'cname'  
  选项cname'ftp.example.com'  
  期权目标'www.example.com'
```

请注意，有必要使用完全限定的域名。

MX RR

如果您在防火墙后面为您的域运行邮件服务器（因此，对于您自己的域，您可能需要分割），那么您可能需要说服该邮箱对您的域实际是权威的。

如果sendmail告诉您“发件人地址的域名xxx@yyy.zzz不存在”，那是因为没有找到一个MX记录，确认它是该域的MX中继。

添加：

```
config'mxhost'  
  选项域'yyy.zzz'  
  选项继电器'my.host.com'  
  选项pref 10
```

将减轻分裂造成的问题。

TFTP引导

直接BOOTP请求到TFTP服务器的IP地址 192.168.1.2，并 /tftpboot/pxelinux.0 用作引导文件名。

```
config'boot'  
  选项'filename''pxelinux.0'  
  选项'servername''data'  
  选项'serveraddress''192.168.1.2'
```

多个DHCP / DNS服务器/转发器实例

如果您需要具有不同配置的 (Domain Name System)多个DNS (Domain Name System)转发器或具有不同租用文件集的DHCP服务器，请查看此Pull请求 (<https://github.com/lede-project/source/pull/408>)。

 当PR合并时，添加说明。

网络界面（luci）尚未更新此PR。

启用DNS而不启用DHCP

dnsmasq可用于向客户端提供DNS (Domain Name System)服务器，但不能使用DHCP（例如，如果DHCP已由单独的服务器提供）。

首先，内部接口必须打开dnsmasq：

- 网络>接口
 - 单击所需的内部界面进行选择

- DHCP服务器
 - 单击“设置DHCP服务器”按钮在此界面上启用dnsmasq - 这将启用DHCP和DNS (Domain Name System)

现在启用了dnsmasq，需要关闭dnsmasq的DHCP部分。

- 网络>接口
 - 单击所需的内部界面进行选择
 - DHCP服务器
 - 忽略接口：启用此选项
 - 保存并申请

此更改将仅关闭DHCP，但在指定的界面上可以使DNS (Domain Name System)服务可用。

几个DNS服务器

```
config dnsmasq
    选项domainneeded'1'
    选项localise_queries'1'
    选项本地'/ lan /'
    选项域'lan'
    选项expandhosts'1'
    选项权威'1'
    选项readethers'1'
    option leasefile'/tmp/dhcp.leases'
    选项resolvfile'/tmp/resolv.conf.auto'
    列表服务器'/subdomain.example.com/192.0.2.1'
    #be注意一些选项应该不存在（或设置为False）
    # 允许转发到“如此定义”的专用网络
    #http: //en.wikipedia.org/wiki/Private_network
    #可能'bogusprivat'
    列表服务器'/example.com/208.67.222.222'
    选项rebind_protection'0'
```

Windows Active Directory域/ DNS依赖目录的认证服务的条件DNS转发

1.使用本地软件包管理器安装dnsmasq

2.编辑/etc/dnsmasq.conf

```
# 告诉dnsmasq将remote.local域中的任何东西转发到dns（示例）服务器10.25.11.2: server
= / remote.local / 10.25.11.2
```

```
# 只听来自本地机器的请求:
```

```
listen-address = 127.0.0.1
```

```
# 不要缓存任何东西 # 一个体面的dns服务器已经为您的本地网络缓存:
```

```
cache-size = 0
```

3.编辑/etc/resolv.conf

```
# 本地局域网 (Local Area Network)域名:
```

```
域名ion.lan
```

```
# local dnsmasq server:
```

```
nameserver 127.0.0.1
```

```
# 您的主要dns服务器（dnsmasq将所有请求转发到此示例服务器）：
```

```
nameserver 10.20.1.1
```

4.启动dnsmasq

5.使用FQDN测试本地服务器和远程服务器

所有dns请求将被转发到10.20.1.1，除了任何匹配的*.remote.local。server.remote.local将转发到10.25.11.2

信用：[http \(http://pyther.net/2010/12/dns-conditional-forwarding-dnsmasq/\)](http://pyther.net/2010/12/dns-conditional-forwarding-dnsmasq/)：

[//pyther.net/2010/12/dns-conditional-forwarding-dnsmasq/](http://pyther.net/2010/12/dns-conditional-forwarding-dnsmasq/) (<http://pyther.net/2010/12/dns-conditional-forwarding-dnsmasq/>)

```
cat / etc / config / dhcp

config dnsmasq
    选项localise_queries'1'
    选项rebind_protection'0'
    选项权威'1'
    option leasefile '/tmp/dhcp.leases'
    option localservice'1'
    选项dnssec'0'
    选项cachesize'0'
    选项域'example.local'
    选项readethers'1'
    选项logqueries'1'
    选项fliterwin2k'0'
    # 在这里定义您的域和域控制器IP地址。
    选项本地 '/example.local/192.168.1.X'n
    列表服务器 '/0.openwrt.pool.ntp.org/8.8.8.8'
    列表服务器 '/1.openwrt.pool.ntp.org/8.8.8.8'
    列表服务器 '/2.openwrt.pool.ntp.org/8.8.8.8'
    列表服务器 '/3.openwrt.pool.ntp.org/8.8.8.8'
    选项resolvfile '/etc/resolv.conf'
    选项boguspriv'1'

config dhcp'lan'
    选项界面'lan'
    选项开始'100'
    期权限额'150'
    选项leasetime'12h'
```


几乎完成了，现在完成/etc/resolv.conf的定义传统上，/etc/resolv.conf通过符号链接填充，基于通过脚本插入到/tmp/resolv.conf中的接口设置。我们要禁用这个符号链接，因为没有这样做会覆盖我们的静态设置。

您将要删除/etc/resolv.conf这将删除resolv.conf符号链接。然后，我们将在/etc/resolv.conf文件中添加辅助DNS (Domain Name System)和外部解析地址的IP地址，最终建立条件转发，应该通过GUI (Graphical User Interface)轻松配置。

```
rm /etc/resolv.conf
echo"domain example.local">> / etc / resolv.conf
echo"nameserver 127.0.0.1">> / etc / resolv.conf
echo"nameserver 208.67.220.220">> / etc / resolv.conf
```

```
cat /etc/resolv.conf
# 定义您所需的域名&公共DNS。
```

```
域名example.local
名称服务器127.0.0.1
名称服务器208.67.220.220
```

 最后修改：2017/02/12 01:05 由ericluehrsen

除非另有说明，本维基的内容将根据以下许可证获得许可：CC Attribution-Share Alike 4.0 International
(<http://creativecommons.org/licenses/by-sa/4.0/>)