

DHCP配置

DHCP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

类型的节 `dnsmasq` 指定每个`dnsmasq`实例与所有接口上的`dnsmasq`实例和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：

```
root @ lede: /#uci show dhcp
DHCP.@的dnsmasq [0] =的dnsmasq
DHCP.@的dnsmasq [0] .domainneeded = '1'
DHCP.@的dnsmasq [0] .boguspriv = '1'
DHCP.@的dnsmasq [0] .filterwin2k = '0'
DHCP.@的dnsmasq [0] .localise_queries = '1'
DHCP.@的dnsmasq [0] .rebind_protection = '1'
DHCP.@的dnsmasq [0] .rebind_localhost = '1'
DHCP.@的dnsmasq [0] .本地= '/ LAN /'
DHCP.@的dnsmasq [0] .域= 'LAN'
DHCP.@的dnsmasq [0] .expandhosts = '1'
DHCP.@的dnsmasq [0] .nonegcache = '0'
DHCP.@的dnsmasq [0] .authoritative = '1'
DHCP.@的dnsmasq [0] .readethers = '1'
DHCP.@的dnsmasq [0] .leasefile = '/ TMP / dhcp.leases'
DHCP.@的dnsmasq [0] .resolvfile = '/ TMP / resolv.conf.auto'
DHCP.@的dnsmasq [0] .localservice = '1'
...
```

```

root @ lede: /# cat / etc / config / dhcp
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 1
    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
add_local_domain	布尔	1		将resolv.conf中的本地域添加为搜索指令。
add_local_hostname	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 add_local_fqdn
add_local_fqdn	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 - iface.host.domain 所有地址。 ⚠ add_local_fqdn 在中继，但不是17.01.0
add_wan_fqdn	整数	0		标签WAN接口， add_local_fqdn 而不是您的ISP分配的默认值，这可能是模糊的。 WAN从 config dhcp 具有 option ignore 1 集合的部分推断出来，因此不需要在中继线上命名为WAN ⚠ add_wan_fqdn ，而不是17.01.0
addnhosts	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
authoritative	布尔	1	-K	强制dnsmasq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
bogusnxdomain	IP地址列表	（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 System)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dnsmasq。
cachesize	整数	150	-c	尺寸的dnsmasq查询缓存。
dbus	布尔	0	-1	启用dnsmasq的DBus消息传递。dnsmasq的 ⚠标准版本不包括DBus支持。

dhcp_boot	串	(没有)	-dhcp-boot	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 “
dhcphostsfile	文件路径	(没有)	-dhcp-hostsfile	使用每个主机DHCP选项指定一个外部文件
dhcpleasemax	整数	150	-X	DHCP租约的最大数量
dnsforwardmax	整数	150	-0 (零)	最大并发连接数
domain	域名	(没有)	-s	DNS (Domain Name System)域发送给DHCP客户端
domainneeded	布尔	1	-D	告诉dnsmasq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	-dnssec	验证DNS (Domain Name System)回复并缓存DNSSEC数据。 ⚠需要dnsmasq-full包。
dnsseccheckunsigned	布尔	0	-dnssec-check-unsigned	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DNS (Domain Name System)区域的未签名回复，但是较慢，并且要求dnsmasq上游的名称服务器具有DNSSEC能力。 ⚠需要dnsmasq-full包。 ⚠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，dns解析可能会在设备重启后中断。
ednspacket_max	整数	1280	-P	指定DNS (Domain Name System)转发器支持的最大EDNS.0 UDP数据包
enable_tftp	布尔	0	-enable-tftp	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 <code>/etc/hosts</code>
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	-dhcp-fqdn	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, dnsmasq 将侦听除列出的所有接口之外的所有接口 notinterface 。请注意, dnsmasq 默认监听环回。
leasefile	文件路径	(没有)	-l (小写字母“L”)	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 <code>/etc/hosts</code> 。这与 server 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 <code>/etc/hosts</code> 。  请注意此选项的拼写。
localservice	布尔	1	-local-service	接受DNS (Domain Name System)只能从主机地址为本地子网中的查询, 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, 存储缓存在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 <code>/etc/hosts</code>
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 <code>/etc/resolv.conf</code>
notinterface	接口名称	(没有)	-I (大写)	接口 dnsmasq 不应该监

	列表		字母“i”)	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	-stop-dns-rebind	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	-rebind-localhost-ok	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
rebind_domain	域名列表	(没有)	-rebind-domain-ok	允许RFC1918响应的域列表仅在启用重新绑定保护时生效
resolvfile	文件路径	/etc/resolv.conf	-r	指定一个替代的resolv文件
server	字符串列表	(没有)	-S	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。
strictorder	布尔	0	-o	服从DNS (Domain Name System)服务器的顺序 /etc/resolv.conf
tftp_root	目录路径	(没有)	-tftp-root	指定TFTP根目录
minport	整数	0	-min-port	Dnsmasq选择随机端口作为出站查询的源。当给出此选项时，所使用的端口

				将始终大于或等于指定的 minport 值（最小有效值 1024 ）。适用于防火墙后面的系统。
maxport	整数	0	-max-port	Dnsmasq 选择随机端口作为出站查询的源。当给出此选项时，所使用的端口将始终小于或等于指定的 maxport 值（最大有效值 65535 ）。适用于防火墙后面的系统。
noping	布尔	0	-no-ping	默认情况下， dnsmasq 会通过将 ICMP 回显请求（也称为 ping ）发送到相关地址，来检查 IPv4 地址是否正在使用，然后再分配给主机。此参数允许禁用此检查。
allservers	布尔	0	-all-servers	默认情况下，当 dnsmasq 有多个上游服务器可用时，它将只向一个服务器发送查询。设置此参数将强制 dnsmasq 将所有查询发送到所有可用的服务器。首先应答的服务器的回复将返回给原始请求者。
quietdhcp	布尔	0	-quiet-dhcp	禁止记录 DHCP 的日常操作。错误和问题仍将被记录
sequential_ip	布尔	0	-dhcp-sequential-ip	Dnsmasq 旨在使用客户端 MAC 地址的散列来为 DHCP 客户端选择 IP 地址。这通常允许客户端的地址长期保持稳定，即使客户端有时允许其 DHCP 租约过期。在此默认模式下， IP 地址在整个可用地址范围内伪随机分布。有时情况（通常是服务器部署），从最低可用地址开始，顺序地分配 IP 地址更方便，并且设置此参数可启用此模式。请注意，在顺序模式下，允许租期过期的客户端更有可能移动

				IP地址; 由于这个原因, 它不应该被普遍使用。
addmac	[0,1, BASE64, 文本]	0	-add-mac	将请求者的MAC地址添加到上游转发的DNS (Domain Name System) 查询; 这可以用于上游服务器进行DNS (Domain Name System)过滤。 如果请求者与dnsmasq服务器位于同一子网上, 则只能添加MAC地址。请注意, 用于实现此目的的机制 (EDNS0选项) 尚未标准化, 因此应将其视为实验性的。另请注意, 以这种方式暴露MAC地址可能会带来安全隐患。
logdhcp	布尔	0	-log-dhcp	启用额外的DHCP日志记录; 记录发送到DHCP客户端的所有选项以及用于确定它们的标签

DHCP池

类型的部分 `dhcp` 指定每个接口租用池和服务DHCP请求的设置。通常, 文件中至少有一个这样的部分存在于 `/etc/config/dhcp` 文件中以覆盖lan接口。

您可以通过指定 `ignore` 相应部分中的选项来禁用特定接口的租用池。

部分的一个最小例子 `dhcp` 如下所示:

```
config 'dhcp' 'lan'
    选项 'interface' 'lan'
    选项 '开始' '100'
    选项 'limit' '150'
    选项 'leasetime' '12h'
    选项 ra 服务器
    选项 dhcpv6 服务器
```

- `lan` 指定此DHCP池提供的接口
- `100` 是与网络地址的偏移量, 在默认配置中, 这意味着开始租用地址 `192.168.1.100`
- `150` 是可以租用的最大地址数, 在默认配置中, 这意味着租用地址 `192.168.1.250`
- `12h` 在这个例子中规定了12个小时的租赁时间
- `server` 定义IPv6配置模式 (RA&DHCPv6)

以下是 `dhcp` 部分法律选项的列表。

		需	
--	--	---	--

名称	类型	要	默认	描述
dhcp_option	字符串列表	没有	(没有)	此处的ID dhcp_option必须用下划线写入。它将被转换为-dhcp-option，带有连字符，最终由dnsmasq使用。可以为此网络ID给出多个选项值，它们之间有一个空格和“”之间的总字符串。例如'26, 1470'或'选项: mtu, 1470'，可以为每个DHCP分配一个MTU。您的客户端必须通过DHCP接受MTU才能正常工作。 或“3,192.168.1.1 6,192.168.1.1”发出网关和dns服务器地址。
dynamicdhcp	布尔	没有	1	动态分配客户端地址，如果设置为 0 仅提供ethers 文件中存在的客户端
force	布尔	没有	0	即使在同一网段上检测到另一个DHCP服务器，也强制在指定接口上进行DHCP服务
ignore	布尔	没有	0	指定是否的dnsmasq如果设置为应忽略这个游泳池 1
dhcpv4	串	没有	none	指定是否启用 none 或禁用DHCPv4服务器 (disabled)
dhcpv6	串	没有	none	指定是否应启用DHCP服务器 (server)，中继 (relay) 或禁用 (disabled)
ra	串	没有	none	指定是否启用路由器广告 (server)，中继 (relay) 或禁用 (disabled)
ndp	串	没有	none	指定是否中继NDP relay 或禁用 none
master	布尔	没有	0	指定中继模式下DHCPv6，RA和NDP是否为主接口。
interface	逻辑接口名称	是	(没有)	指定与此DHCP地址池关联的接口; 必须是其中定义的接口之一 /etc/config/network 。
leasetime	串	是	12h	指定发送给客户端的地址的租用时间，例如 12h 或 30m
limit	整数	是	150	指定地址池的大小 (例如start = 100, limit = 150, 最大地址为.249)
networkid	串	没有	(价值 interface)	dhcp部分中定义的dhcp功能仅限于此处通过其network-id指定的接口。如果系统通过/ etc / config / network的协商尝试通过此dhcp部分中的“接口”设置来知道网络ID。一些ID动态分配，不由网络提供，但仍可在此设置。
start	整数	是	100	指定与底层接口的网络地址的偏移量，以计算出租给客户端的最小地址。跨越子网可能大于255。

instance	dnsmasq 实例	没 有	（没有）	dhcp部分绑定到的Dnsmasq实例; 如果没有指定 该部分对所有dnsmasq实例有效。
----------	---------------	--------	------	---

笔记:

- 虽然称为“接口”，这是网络名称，即lan，wan，wifi等（/ etc / config / network中的段名称），而不是内部使用的接口名称，如eth0，eth1，wlan0等（“ / etc / config / network中的ifname'ID”）。
- 虽然称为“networkid”，这是内部使用的接口名称，即eth0，eth1，wlan0等，而不是网络名称（lan，wan，wifi等）。

这在/ etc / config / network和/ etc / config / wireless中使用的'ifname'和'network'偏离，所以双重检查！

静态租赁

您可以根据其MAC（硬件）地址，为网络上的主机分配固定的IP地址。

本节中的配置 -G 选项用于构建 dnsmasq的选项。

配置主机

```
选项ip'192.168.1.2'  
选项mac '00: 11: 22: 33: 44: 55'  
选项名称'mypc'
```

这将为（以太网）硬件地址00: 11: 22: 33: 44: 55的机器添加固定IP地址192.168.1.2和名称“mypc”。

配置主机

```
选项ip'192.168.1.3'  
option mac '11: 22: 33: 44: 55: 66 aa: bb: cc: dd: ee: ff'  
选项名称“mylaptop”
```

这将为（以太网）硬件地址11: 22: 33: 44: 55: 66或aa: bb: cc: dd: ee: ff的机器添加固定IP地址192.168.1.3和名称“mylaptop”。请注意，如果列出的多个mac地址同时在网络上，则这是不可靠的。这对于具有无线和有线接口的笔记本电脑的情况非常有用，只要在给定时间只有一个将处于活动状态。

名称	类型	需要	默认	描述
ip	串	是	（没有）	“忽略”或要用于此主机的IP地址。
mac	串	没有	（没有）	该主机的硬件地址（以逗号分隔）。
hostid	串	没有	（没有）	IPv6接口标识符（地址后缀）为十六进制数（最多8个字符）
duid	串	没有	（没有）	该主机的DHCPv6-DUID。

name	串	没有	(没有)	要分配的可选主机名。
tag	串	没有	(没有)	设置匹配主机的给定标签。
dns	布尔	没有	0	为此主机添加静态正向和反向DNS (Domain Name System) 条目。
broadcast	布尔	没有	0	强制广播DHCP响应。
leasetime	串	没有	(没有)	主机特定的租用时间，例如2m，3h，5d。注意：由r48801在后备箱中引入
instance	dnsmasq实例	没有	(没有)	主机部分绑定到的Dnsmasq实例; 如果没有指定该部分对所有dnsmasq实例有效。

DHCP OPTION示例设置备用默认网关

您可以指定备用的默认网关

```
config'dhcp''lan'
    选项'interface''lan'
    选项'开始''100'
    选项'limit''150'
    选项'leasetime''12h'
    list'dhcp_option''3,192.168.1.2'
```

使用列表'dhcp_option"3,192.168.1.2'设置默认网关。一个选项列表可以在这里找到 [这里](http://www.networksorcery.com/enp/protocol/bootp/options.htm) (<http://www.networksorcery.com/enp/protocol/bootp/options.htm>)

启动选项

一些主机支持通过网络引导（PXE引导）。DHCP / BOOTP用于告诉主机要启动哪个文件，服务器将其加载。每个客户端只能接收一组文件名和服务器地址选项。如果不同的主机应该引导不同的文件，或者从不同的服务器启动，可以使用网络ids将选项映射到每个客户端。

通常，您需要为 dhcp_option 启动过程的进一步阶段设置其他DHCP选项（通过）。有关该选项的语法的详细信息，请参阅dnsmasq手册页 0。

本节中的配置 -M 选项用于构建 dnsmasq的选项。

注: odhcp目前缺少支持根路径规范。如果需要此功能，请禁用odhcpd并使用dnsmasq。

```
配置启动linux
    选项文件名'/tftpbboot/pxelinux.0'
    option serveraddress'192.168.1.2'
    选项servername'fileserver'
    list dhcp_option'选项: root-path, 192.168.1.2: / data / netboot / root'
```

这将告诉客户端从服务器加载pxelinux.0到192.168.1.2，并从 / data / netboot / root安装在同一台服务器上。

名称	类型	需要	默认	描述
dhcp_option	字符串列表	没有	(没有)	为此网络ID添加的其他选项。⚠️如果指定了这一点，您还需要指定network-id。
filename	串	是	(没有)	主机应该从引导服务器请求的文件名。
networkid	串	没有	(没有)	这些启动选项应该适用的网络ID。如果未指定，则适用于所有客户端。
serveraddress	串	是	(没有)	引导服务器的IP地址。
servername	串	是	(没有)	引导服务器的主机名。
force	布尔	没有	(没有)	始终发送dhcp-option，即使客户端在参数请求列表中没有要求它。这有时需要，例如向PXELinux发送选项时。
instance	dnsmasq实例	没有	(没有)	引导部分绑定到的Dnsmasq实例; 如果没有指定该部分对所有dnsmasq实例有效。

分类客户和分配个别选项

DHCP可以为客户端提供多种选项，如域名，NTP服务器，网络引导选项等。虽然某些设置适用于网段中的所有主机，但其他设置更具体，仅适用于一组主机，甚至只有一个。*dnsmasq*提供通过网络ID，字母数字标识符将DHCP选项及其值分组，并仅向已标记有该网络标识的主机发送选项。

您可以通过他们所在的DHCP范围（部分 dhcp ）标记主机，或者客户端可以使用其DHCP请求发送的多个选项。在每个这些部分中，您可以使用 dhcp_option 列表添加要使用此网络ID发送到主机的DHCP选项。

每个分类部分都有两个配置选项：用于区分客户端的DHCP选项的值以及这些客户端应标记的网络ID。这是一个模板：

```
config classifier option classifier 'value' option networkid 'network-id' list
dhcp_option 'DHCP-option'
```

占位符 *classifier* 可以是以下值之一：

分类	描述
mac	客户端的硬件地址
vendorclass	由客户端发送的字符串代表客户端的供应商。 <i>dnsmasq</i> 使用此值对供应商类字符串执行子串匹配。
userclass	由客户端发送的表示客户端用户的字符串。 <i>dnsmasq</i> 使用此值对用户类字符串执行子串匹配。

circuitid	匹配中继代理发送的电路ID，如RFC3046所定义。
remoteid	匹配中继代理发送的远程ID，如RFC3046所定义。
subscrid	匹配中继代理发送的用户ID，如RFC3993中定义的。

使用“mac”分类器为openvpn创建标记网络的示例将在配置文件中看起来像这样：

```
config mac 'opnvpn'
    选项mac '00: FF: *: *: *: *'
    选项networkid 'opnvpn'
    列表dhcp_option '3'
```

在UCI中也是这样

```
dhcp.opnvpn = MAC
dhcp.opnvpn.mac = 00: FF: *: *: *: *
dhcp.opnvpn.networkid = opnvpn
dhcp.opnvpn.dhcp_option = 3
```

DHCP选项为此网络ID添加DHCP选项。有关该选项的语法的完整说明，请参阅*dnsmasq*手册页 - 0。

力是一个bool选项。它强制dhcp_option始终被发送，即使客户端没有在参数请求列表中要求它。这有时需要，例如向PXELinux发送选项时。

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
```

DHCP端口

DHCP需要从您的区域到/从防火墙打开UDP端口67和68。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

静态租赁（MAC地址热插拔）

定义静态租赁与MAC地址的主机 `00:a0:24:5a:33:69` 和 `00:11:22:33:44:55`（方便当你使用在同一台计算机/笔记本电脑的有线和无线连接-当然，你可以只使用一个MAC地址）和分配的IP地址 `192.168.1.230` 和主机名 `example-host` 到它。我们称这个MAC地址热插拔，因为IP地址保持不变，但MAC地址发生变化。

```
config'host'
  选项'name''example-host'
  option'ip''192.168.1.230'
  选项'mac''00: a0: 24: 5a: 33: 69 00: 11: 22: 33: 44: 55
```

故障排除

🚨 **Windows 7** 引入了一个新的 *Microsoft* 增强功能。即使该接口当前没有激活（即断开电缆），也不会将从DHCP服务器获取的IP地址分配给接口。此行为是唯一的，并没有针对较旧的Windows版本，Mac OS (Operating System) 和Linux报告。

如果您尝试在路由器上配置MAC地址热插拔，则Windows 7客户端将以无限DORA (<http://tools.ietf.org/html/rfc1531#section-3.1>) 循环结束。

解：

1. 从客户端的无线和以太网接口创建一个桥
 - 这是微不足道的：谷歌它 (<https://www.google.com/search?q=windows%20%20create%20bridge&btnl=lucky>)
 - 您将必须添加桥的MAC地址 `/etc/config/dhcp`

```
config'host'
  选项'name''example-host'
  option'ip''192.168.1.230'
  选项'mac''00: a0: 24: 5a: 33: 69 00: 11: 22: 33: 44: 55 02:
a0: 24: 5a: 33: 69 02:11:22:33:44:55
```

- 由于桥接器可能会改变您的以太网MAC地址，所以您将失去WiFi接口上的SLAAC，从而使您的笔记本电脑在无线连接时禁用IPv6。
2. 另一种解决方案是IPv6友好，您不需要创建一个网桥，也不需要为dnsmasq配置文件添加MAC地址，但它涉及用户交互：
 - 当您插入以太网电缆时，禁用控制面板中的无线接口（无线功能将不会这样做）。
 - 拔掉以太网电缆后，启用无线和禁用以太网。

笔记：

- http://answers.microsoft.com/en-us/windows/forum/windows_7-networking/windows-7-refuses-dhcp-addresses-if-they-were/1b72b289-0f58-492f-afb8-e76c80a81f00 (http://answers.microsoft.com/en-us/windows/forum/windows_7-networking/windows-7-refuses-dhcp-addresses-if-they-were/1b72b289-0f58-492f-afb8-e76c80a81f00)
- *force* 是一个bool选项，将强制dhcp-option始终发送，即使客户端不在参数请求列表中要求它。这有时需要，例如向PXELinux发送选项时。

只允许静态租赁

如果要仅将IPv4地址分配给已知客户端（静态租约），请使用：

```
config dhcp 'lan'
...
选项dynamicdhcp 0
```

因此，dnsmasq将考虑在“config host”块和/ etc / ethers中定义的静态租约，并拒绝向未知客户端发出任何IPv4地址。

请注意，您不应将此作为安全功能，以防止不必要的客户端连接。客户端可以简单地配置正确范围内的静态IP以访问网络。

多个DHCP选项

可以在单个dhcp_option对象下配置多个DHCP选项。在这种情况下，Cisco Callmanager部署使用了选项66（tftp-server）和选项150（多个tftp服务器）。

```
config 'dhcp' 'lan'
  选项 'interface' 'lan'
  选项 '开始' '62'
  选项 'limit' '192'
  选项 'leasetime' '600h'
  列表 'dhcp_option' '66, 172.16.60.64'
  list 'dhcp_option' '150, 172.16.60.64'
```

多个DHCP / DNS服务器/转发器实例

运行多个dnsmasq实例作为DNS (Domain Name System)转发器和/或DHCPv4服务器，每个具有自己的配置和租赁列表可以通过创建多个dnsmasq部分进行配置。

通常在这样的配置中，每个dnsmasq部分将通过使用 interface 列表绑定到特定的接口；将这些部分（如dhcp，host等）分配给特定的dnsmasq实例是由参数完成的 instance 。默认情况下，dnsmasq将Loopback接口添加到接口列表中，以便在使用该 -interface 选项时侦听；因此，通过使用 notinterface 列表，需要在其中一个dnsmasq实例中排除环回接口。

这些是多个dnsmasq实例的示例设置，每个实例都有自己的dhcp部分；dnsmasq 实例主要绑定到 lan接口，而dnsmasq 实例来宾绑定到访客接口：

```
config dnsmasq'main'
    选项domainneeded'1'
    选项boguspriv'1'
    选项filterwin2k'0'
    选项localise_queries'1'
    选项rebind_protection'1'
    选项rebind_localhost'1'
    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nonwildcard'1'
    列表界面'lan'

config dnsmasq'guest'
    选项domainneeded'1'
    选项boguspriv'1'
    选项filterwin2k'0'
    选项localise_queries'1'
    选项rebind_protection'1'
    选项rebind_localhost'1'
    选项本地'/ guest /'
    选项域'guest'
    选项expandhosts'1'
    选项nonegcache'0'
    选项权威'1'
    选项readethers'1'
    option leasefile'/tmp/dhcp.leases.guest'
    选项resolvfile'/tmp/resolv.conf.guest'
    选项strictorder'1'
    选项nonwildcard'1'
    列表界面“访客”
    列表notinterface'lo'

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

config dhcp'guest_private'
    选项实例'guest'
    选项界面'guest'
    选项开始'100'
    期权限额'150'
    选项leasetime'12h'

...
```


Web界面（luci）尚未更新，以支持多个dnsmasq实例。

将DHCP池分配给大型网络中的子网

在DHCP池限制设置中，启动和限制值不*参考“最后一个数字”，它们是网络地址的相对偏移量。

- 10.0.0.1 / 255.0.0.0的网络地址为10.0.0.0
- 10.22.0.1起始地址为22 x / 16个子网： $(2^{16}) * 22 = 1441792$
- $10.0.0.0 + 1441792 + 1 = 10.22.0.1 \rightarrow \text{start} = 1441793$
- $10.22.0.254 - 10.22.0.1 = 253 \rightarrow \text{limit} = 253$

```
config dhcp lan
    选项界面lan
    选项开始1441793
    选项限制253
```

测试：

```
root @ lede: ~# ipcalc.sh 10.0.0.1 255.0.0.0 1441793 253
IP = 10.0.0.1
NETMASK = 255.0.0.0
BROADCAST = 10.255.255.255
网络= 10.0.0.0
PREFIX = 8
START = 10.22.0.1
END = 10.22.0.254
```

分类客户和分配个别选项

将不同的dhcp选项分配给单个MAC地址：

```
uci批<<“EOF”
添加dhcp mac
设置dhcp.@ mac [-1] .mac = 00: 11: 22: 33: 44: 55
设置dhcp.@ mac [-1] .networkid =某人
add_list dhcp.@ mac [-1] .dhcp_option = 6,192.168.1.3,192.168.1.2,192.168.1.1
add_list dhcp.@ mac [-1] .dhcp_option = 3,192.168.1.2
add_list dhcp.@ mac [-1] .dhcp_option = 44,192.168.1.3
提交dhcp
EOF
uci commit dhcp
/etc/init.d/dnsmasq重新加载
```

其中6 = DNS (Domain Name System), 3 =默认网关, 44 = WINS

为多个主机分配不同的dhcp选项：

配置主机

选项名称“j400”

选项mac '00: 21: 63: 75: aa: 17'

选项ip '10 .11.12.14'

选项标签'vpn' # 将标签“vpn”分配给此主机

配置主机

选项名称'j500'

选项mac '01: 22: 64: 76: bb: 18'

选项ip '10 .11.12.15'

选项标签'vpn' # 将标签“vpn”分配给此主机

```
config tag'vpn'#match tag“vpn”
```

```
list dhcp_option'6,8.8.8.8,8.8.4.4'#将arbitrary extra dhcp选项分配给此标签
```

选项强制'1' # dhcp-option将始终发送，即使客户端不在参数请求列表中要求它。这有时需要，例如向PXELinux发送选项时。

⚠通常，指定没有任何值的dhcp选项将禁用该选项。所以例如你可以使用：

```
列表dhcp_option'3'
```

禁用向默认的客户发送默认网关

启用DHCP而不启用DNS

当您只想向客户端发送地址，而不执行任何DNS (Domain Name System)时，这是有用的。

```
config dnsmasq
```

```
...  
选项端口0  
选项域“
```

第二个选项可以防止dnsmasq 向客户端发出域名和DNS (Domain Name System)搜索列表：如果没有DNS解析，(Domain Name System)这是无用的。

当然，您将要DNS (Domain Name System)解析器的地址发送给客户端：

```
config dhcp lan
```

```
选项界面lan
```


```
...  
list dhcp_option“6,80.67.188.188,6,80.67.169.12”  
list dns“2001: 913 :: 8”  
list dns“2001: 910: 800 :: 12”
```

`dhcp_option`条目适用于dnsmasq，而更优雅的`dns`条目被odhcpd理解。默认情况下，odhcpd仅用于IPv6，但是如果您还使用odhcpd作为IPv4，那么只需使用“dns”条目即可。

故障排除

当网络超载时，由于缺少dhcp响应而导致连接丢失

有时，当接口处于容量边缘（特别是较长距离的wifi）时，dhcp请求可能无法及时回复，因此dhcp客户端将无法接收正确的网络设置。可能的解决方法是使用静态IP或非常长的dhcp租约（超过12h）。当具有使用dhcp并且彼此远离或不容易访问的多个WiFi中继器时，这尤其重要。

 最后修改：2017/02/12 01:21 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/>)