DNSMASQ HOWTO

Dnsmasq e' un software che eroga i servizi dhcp e dns. La presente guida non vuole essere completa, e' soltanto la somma degli appunti cui mi sono rifatto per rendere operativo il servizio.
Nella presente guida la distribuzione di riferimento e' slackware 12 [la prima, l'unica :-)], ove il software e' gia' correttamente installato. Non analizzeremo quindi la procedura di compilazione partendo dai sorgenti. Una panoramica generale su dnsmasq possiamo leggerla a questo link [in inglese] :

http://en.wikipedia.org/wiki/Dnsmasq

dnsmasq accetta query dns e risponde utilizzando una sua cache, se cio' non e' sufficiente allora interroga altri dns. Come impostazione predefinita legge il file /etc/hosts ed utilizza le informazioni qui presenti. Potrebbe essere quindi una buona soluzione utilizzare il file /etc/hosts per "mappare" una lan, dnsmasq provvedera' poi a fornire il servizio in base alle direttive presenti. Il server DHCP di dnsmasq supporta un assegnamento statico agli host, reti multiple, DHCP-relay e RFC3011 subnet specifiers. Dnsmasq comprende un server TFTP sicuro per consentire il boot net/PXE. Supporta anche BOOTP . Supporta ipv6 per le richieste dns, ma non utilizza ipv6 come assegnazione dhcp.
Su slackware 12 il servizio parte al boot del sistema, a patto che lo script di avvio possieda l'attributo di eseguibilita'; in questo modo:

-rwxr-xr-x 1 root root 512 2007-04-30 00:29 rc.dnsmasq

Il percorso completo dello script e' /etc/rc.d/rc.dnsmasq .
Per avviare il servizio occorre la seguente sintassi:

/etc/rc.d/rc.dnsmasq start

 se vogliamo fermare il servizio allora digiteremo:

 /etc/rc.d/rc.dnsmasq stop

infine per il riavvio del servizio digiteremo:

/etc/rc.d/rc.dnsmasq restart

dnsmasq adegua il suo comportamento in base alle direttive del file di configurazione /etc/dnsmasq.conf. Tale file ha l'aspetto solito dei files di configurazione dei sistemi linux. E un file di testo piano, ove ogni linea e' una direttiva. I commenti iniziano col carattere # ed ovviemente non modificano il comportamento del servizio. Le direttive possibili all'interno di dnsmasq.conf sono parecchie. Il file presente di default e' ampiamente commentato e vi sono molte configurazioni possibili. Possiamo utilizzare due criteri per scrivere le direttive.
fare riferimento a:

http://www.faqs.org/rfcs/rfc2132.html

ed utilizzare il sistema numerico oppure possiamo utilizzare la notazione estesa. dnsmasq interpretera' entrambe. Se vogliamo utilizzare la notazione numerica allora ci viene in aiuto un elenco completo di tale notazione:

http://www.networksorcery.com/enp/protocol/bootp/options.htm.

In alternativa possiamo lanciare il seguente comando

dnsmaqs --help dhcp

il quale ci restituisce tutte le possibili direttive.
Ecco un esempio di configurazione utilizzando la notazione numerica:

```
dhcp-option=3,192.168.35.1        # indichiamo il default gateway
dhcp-option=6,192.168.35.10       # dns da passare ai client
dhcp-option=1,255.255.255.0       # indica la netmask
dhcp-option=44,172.16.0.3         # indica il server wins
dhcp-option=46,8                  # indica il tipo nodo
dhcp-option=42,193.204.114.105  # indica il server ntp
```

Segue una traduzione parziale del file dnsmasq.conf, cosi' come e' presente all'atto dell'installazione di slackware 12.

domain-needed	ignora i nomi host privi del punto e dell'estensione di dominio, e non propaga le informazioni ad essi riferite. (non inoltrare mai ai server dns esterni query senza nome dominio)
filterwin2k	Filtra le ricorrenti richieste SOA, SRV e altre, provenienti da macchine windows serve in particolare a non attivare per sbaglio il link quando si hanno connessioni "on demand"
strict-order	impostando questa direttiva indichiamo a dnsmasq di consultare i dns di appoggio esattamente nell'ordine in cui appaiono nel file /etc/resolv.conf
bogus-priv	non propaga gli indirizzi riferiti a zone non routabili. In pratica Tutti i reverse lookup per la subnet privata non presenti in /etc/hosts o nei lease dhcp ottengono “host not found" invece di essere inoltrati ai dns esterni
/etc/resolv.conf	indica dove ottenere i corretti dns cui fare riferimento.
no-resolv	decommentando tale direttiva otteniamo che il servizio dnsmasq non si appoggi al contenuto del file /etc/resolv.conf

server=208.67.222.222 server dns esterni di riferimento inserire i server dns uno per riga. Usati in questo caso i server di opendns.org

expand-hosts aggiunge sempre il nome di dominio al nome host
Es: se un vostro cliente si chiama ``chrome`` e il vostro dominio ``piffa.net`` dnsmasq rendera' disponibile il campo *A* per il dominio ``chrome.piffa.net`` diretto all'ip che verra' assegnato al client. [tratto da: http://doc.andreamanni.com/source/servizi.txt]

domain il nome di dominio sul quale si opera
a) consente di erogare nomi di dominio pienamente qualificati fintanto che la parte del dominio corrisponde a questa impostazione.
b) forza l'impostazione del nome di dominio ai client che ottengono un indirizzo ip (ovviamente da dnsmasq)
c) l'argomento della direttiva domain viene utilizzato come argomento dalla direttiva "expand-hosts"

dhcp-leasefile=/var/lib/dnsmasq/leases posizione del file ove dnsmasq tiene traccia degli indirizzi ip erogati ai client
Possiamo indicare un path differente, a patto di concedere a dnsmasq i permessi di lettura/scrittura sufficienti

dhcp-host=00:18:f8:83:d8:f4,192.168.35.190,LinksysPAP
riserva un determinato ip ad un terminato client la cui scheda di rete possiede il macaddress indicato, ed assegna anche il nome host

log-queries da usare per il debug

resolv-file indica il file contenente i corretti dns da utilizzare. dnsmasq utilizzera' tali indirizzi per la risoluzione dei nomi

no-poll Impedisce che dnsmasq cerchi risoluzioni DNS nei file resolv.conf o altri che siano stati eventualmente modificati

user
group dnsmasq verra' messo in esecuzione coi privilegi dell' utente e del gruppo specificati. Serve a declassare dnsmasq, aumentando la sicurezza

interface indica a dnsmasq su quale interfaccia di rete operare. utile quando l'elaboratore possiede piu' di una scheda di rete

except-interface indica a dnsmasq su quale interfaccia di rete non operare. in pratica dnsmasq non rimane in ascolto sull'interfaccia di rete indicata

listen-address indica a dnsmasq su quale indirizzo ip rimanere in ascolto e quindi erogare i servizi. e' un'alternativa all'utilizzo della direttiva interface

no-dhcp-interface indica a dnsmqasq di non fornire servizio dhcp sull'interfaccia indicata. Verra' erogato solo il servizio dns

local=/localnet/ indicare solo i domini locali. dnsmasq rispondera' alle query per il dominio indicato basandosi esclusivamente sulle informazioni presenti in /etc/hosts , oppure fornira' solo il servizio dhcp

no-hosts indica a dnsmasq di non considerare il file /etc/hosts

addn-hosts indica a dnsmasq di considerare il file indicato al posto di /etc/hosts . In pratica non viene letto /etc/hosts ma il file indicato, ed il contenuto di tale file viene utilizzato da dnsmasq

dhcp-range indica a dnsmasq il range degli indirizzi ip che e' possibile rilasciare. Se dnsmasq opera su piu' di una rete, occorre ripetere la direttiva indicando ogni volta la rere appropriata. Indicare il tempo di lease e' opzionale. Ecco un esempio

dhcp-range=192.168.35.50,192.168.35.100,255.255.255.0,8h

dhcp-host assegna un determinato indirizzo ip ad una determinata scheda di rete appartenente ad un client, identificata tramite mcaddress. Utilizzando tale direttiva e' anche possibile indicare il nome-host da assegnare al client richiedente il lease. Anche il tempo di lease e' quantificabile. interessante la direttiva "ignore" che indica a dnsmasq di ignorare la richiesta di ip proveniente da un determinato mcaddress. Volendo utilizzare tale possibilita' la sintassi corretta diventa la seguente:
dhcp-host=11:22:33:44:55:66,ignore

dhcp-option=3 azzera la route di default, e non sovrascrive alcuna cosa. In pratica la route di default viene annullata. Notare che tale comportamento si ottiene solamente con le opzioni di default (1, 3, 6, 12, 28). con direttive differenti ecco che verra' inviata una stringa nulla

dhcp-option=option:ntp-server,192.168.0.4,10.10.0.5 indica i server del tempo [Time server]

dhcp-option=42,0.0.0.0	indica che il pc NTP time server e' la medesima ove gira dnsmasq
dhcp-option=40,welly	dnsmasq eroghera' come nome di dominio nis " welly "
dhcp-option=23,50	dnsmasq eroghera' come tempo di ttl il valore 50
dhcp-option=27,1	come locali tutte le subnet
dhcp-option = net:red, option:ntp-server, 192.168.1.1	Specifica un'opzione che sara' inviata solamente alla rete "red"
enable-tftp	attiva il trivial ftp server "interno" di dnsmasq
tftp-root=/var/ftpd	indica la directory di lavoro valida per il server ftp “integrato” in dnsmasq
tftp-secure	indicando qst direttiva ecco che solo i files appartenenti a dnsmasq possono essere inviati via rete
dhcp-script=/bin/echo	esegue un particolare comando (non obbligatoriamente /bin/echo) all'atto del rilascio di un lease, oppure all'atto della distruzione di un lease. Verra' inviato come argomento allo script specificato un argomento: "add" all'atto della creazione di un lease, "del" all'atto della distruzione di un lease. Inoltre verranno forniti allo script invocato anche il macaddress, l'indirizzo ip e se possibile anche l'hostname del client richiedente
log-queries	abilita i log riferiti alle richieste di indirizzo ip
log-dhcp	abilita i log riferiti alle transazione dhcp
conf-file=/etc/dnsmasq.more.conf	posizione di un file contenente ulteriori direttive diconfigurazione. In pratica e' possibile fare in modo che dnsmasq adatti il suo comportamento in base al contenuto del file /etc/dnsmasq.conf, il quale a sua volta richiama il file /etc/dnsmasq.more.conf
conf-dir=/etc/dnsmasq.d	legge tutti i file presenti nella posizione /etc/dnsmasq.d , e li utilizza come configurazione
address=/dominio.ext/indirizzo_ip	direttiva utilissima. utilizzando questo comando indichiamo a dnsmasq che il dominio "dominio.net" corrisponde all'indirizzo ip "indirizzo_ip" E' quindi possibile fare una lista di

siti ai quali si vuole proibire l'accesso, ed indicare per questi siti indirizzo ip 127.0.0.1 , di fatto bloccando la navigazione.

ESEMPI DI CONFIGURAZIONE

Seguono ora alcuni esempi di configurazione del servizio. Alcuni di questi esempi sono tratti dalla rete, altri sono stati usati dall'autore durante la stesura del presente.

Esempio numero 1, tratto da
http://wiki.archlinux.org/index.php/ArchSBS_-_DNS_dinamico_e_DHCP

```
addn-hosts=/etc/dnshosts          # legge il file /etc/dnshosts
                                  # che svolge i medesimi compiti
                                  # del file /etc/hosts. Nel senso
                                  # che dnsmasq tratta il file
                                  # /etc/dnshosts esattamente come
                                  # il file /etc/hosts

no-hosts                          # non prende in considerazione
                                  # il file /etc/hosts

local=/mede.it/                   # imposta il dominio mede.it come
                                  # locale. Le query riferita a qst
                                  # dominio saranno evase unicamente
                                  # con le informazioni presenti nel
                                  # file /etc/hosts

interface=eth1                    # indica la scheda di rete ove
                                  # dnsmasq eroghera' i servizi

expand-hosts                      # indica a dnsmasq di completare
                                  # i nomi host  aggiungendo il nome
                                  # di dominio. in qst caso mede.it

domain=mede.it                    # il suffisso di dominio da aggiungere
                                  # ai nomi di host


dhcp-range=192.168.20.50,192.168.20.150,12h     # l'intervallo degli
                                                # indirizzi
                                                # ip da rilasciare ai client

dhcp-option=option:router,192.168.20.1          # l'indirizzo ip del router
                                                # ossia il default gw della
                                                # lan
```

```
dhcp-option=44,192.168.20.1     # set netbios-over-TCP/IP nameserver(s)
                                # aka WINS server(s)

dhcp-option=45,192.168.20.1     # netbios datagram distribution server

dhcp-option=46,8                # netbios node type

dhcp-option=47                  # empty netbios scope.

dhcp-option=6,192.168.20.1      # indica l'indirizzo ip del server dns

mx-host=archi.mede.it,50        # indica un record mx chiamandolo
                                # archi.mede.it
                                # e settando la preferenza a 50

mx-target=archi.mede.it         # imposta archi.mede.it come record mx
                                # predefinito
                                # creato tramite la direttiva localmx

localmx                         # Return MX records for local hosts.

log-queries                     # opzioni utilizzate per il debug del servizio
log-dhcp                        #
```

Esempio numero 2, tratto da
http://siso.sourceforge.net/ap-etc-sysconfig-dnsmasq.html

```
resolv-file=/etc/sysconfig/dnsmasq/resolv.conf      # upstream name
                                                    # servers
no-poll                                             # do not poll resolv-file
except-interface=eth1                               # do not answer on
                                                    # external i/f
domain-needed                                       # don't forward plain
                                                    # names
bogus-priv                                          # don't forward private
                                                    # addresse
bogus-nxdomain=64.94.110.11                         # keep Verisign in control
filterwin2k                                         # filter useless Windows
                                                    # DNS requests
#
# Local DNS name server
#
no-hosts                                            # do not read /etc/hosts
addn-hosts=/etc/sysconfig/dnsmasq/hosts             # instead, read this file
expand-hosts                                        # add the domain to
                                                    # /etc/hosts entries
domain=vonk                                         # domain name
local=/vonk/                                        # answer these domains
                                                    # from /etc/hosts
#
# Automatically configure DHCP client network i/f (RFC 1533)
#
```

```
dhcp-option=1,255.255.255.0                          # subnet mask
dhcp-option=2,-28800                                 # UTC -8:00
dhcp-option=lan, 3,10.0.1.1                          # default g/w for LAN
                                                     # client
dhcp-option=wifi,3,10.0.2.1                          # default g/w for WiFi
                                                     # clients
dhcp-option=vpn, 3,10.0.3.1                          # default g/w for VPN
                                                     # clients
dhcp-option=lan, 6,10.0.1.1                          # DNS server for LAN
                                                     # clients
dhcp-option=wifi,6,10.0.2.1                          # DNS server for WiFi
                                                     # clients
dhcp-option=vpn, 6,10.0.3.1                          # DNS server for VPN
                                                     # clients
dhcp-option=7,10.0.1.2                               # SYSLOG server

#dhcp-option=wifi,33,10.0.1.4,10.0.2.1,10.0.1.100,10.0.2.1 # STATIC ROUTE
                                                           # for WiFi clients

dhcp-option=40,vonk                                  # NIS domain
dhcp-option=41,10.0.1.2                              # NIS domain server
dhcp-option=42,10.0.1.1                              # NTP server
#
# DHCP options for BOOTP
#
#dhcp-option=17,/home/cvonk/tftp                     # BOOTP rootpath
#dhcp-option=18,/pxe/pxelinux.0                      # BOOTP more info
#
# DHCP address range
#
dhcp-range=lan,10.0.1.120,10.0.1.125,,15m            # DHCP addr range for
                                                     # LAN clients
dhcp-range=wifi,10.0.2.120,10.0.2.125,,15m           # DHCP addr range for
                                                     # WIFI clients
# dhcp-range for vpn controlled by L2TP              # DHCP addr rance for
                                                     # VPN clients
#
# MAC addresses below are statically mapped to IP addresses
#
dhcp-host=00:16:76:AA:DE:FF,net:lan,  zoef.vonk,zoef.vonk,24h
dhcp-host=00:90:4B:2F:6E:D4,net:wifi, crox.vonk,crox.vonk,12h
dhcp-host=00:0D:56:32:DD:8B,net:lan,  crox.lan.vonk,crox.lan.vonk,12h
dhcp-host=00:1A:6B:CE:9D:83,net:lan,  bor.lan.vonk,bor.lan.vonk,24h
dhcp-host=00:13:E8:92:4B:5F,net:wifi, bor.vonk,bor.vonk,24h
dhcp-host=00:1d:60:62:28:db,net:wifi, truus.vonk,truus.vonk,12h
dhcp-host=00:1c:23:a1:94:3a,net:lan,  truus.lan.vonk,truus.lan.vonk,12h
dhcp-host=00:17:F2:F9:3D:BA,net:lan,  appletv.vonk,appletv.vonk,24h
dhcp-host=00:1a:73:37:48:1b,net:wifi, myra.vonk,myra.vonk,12h
dhcp-host=00:16:D4:C3:14:E3,net:lan,  myra.lan.vonk,myra.lan.vonk,12h
dhcp-host=00:05:3c:04:b8:65,net:lan,  martha.vonk,martha.vonk,12h
dhcp-host=00:07:95:F9:CF:67,net:lan,  back.vonk,back.vonk,24h
dhcp-host=00:60:08:93:8F:88,net:lan,  nis.vonk,nis.vonk,24h
```

```
#
# MX records
#
# mx-host=vonk,mail.vonk,50                    #
# mx-target=mail.vonk                          # target for localmx
# localmx                                      #
```

Esempio di configurazione utilizzata dall'autore durante la stesura del presente.

```
resolv-file=/etc/resolv.conf          # indica quali dns consultare
domain-needed                         # non inoltra richiese piane, senza
                                      # cioe' il nome dominio
filterwin2k                           # filter useless Windows DNS requests
no-hosts                              # non legge il file /etc/hosts
domain=veronese.local                 # indica il corretto dominio su cui lavorare
local=/veronese.local/                # indica il dominio veronese.local come
                                      # locale
dhcp-option=1,255,255,255,0           # indichiamo la netmask da erogare
dhcp-option=3,10.0.0.1                # indica il default gw
dhcp-option=6,10.0.0.1                # indichiamo il corretto dns
dhcp-range=10.0.0.100,10.0.0.200,15m  # indica il range di ip da assegnare
                                      # ed indica anche il tempo di lease
dhcp-leasefile=/etc/dnsmasq.d/lease   # file che registra gli ip erogati.
```

Un altro esempio creato durante la stesura del presente:

```
no-hosts                              # non considera /etc/hosts
local=/veronese.local/                # imposta il dominio verones.local come locale
interface=eth0                        # imposta la scheda di rete ove erogare il
                                      # servizio
domain=veronese.local                 # imposta il dominio da aggiungere ai nomi host
dhcp-option=option:router,10.0.0.1    # impostiamo il default gw da
                                      # erogare
dhcp-range=10.0.0.100,10.0.0.200,6h   # impostiamo il range di ip da
                                      # utilizzare per l'assegnazione ed
                                      # indichiamo anche il
                                      # tempo di lease
dhcp-option=6,10.0.0.1                # indica il server dns
dhcp-option=44,10.0.0.1               # indichiamo il wins server
dhcp-option=46,8                      # NetBIOS over TCP/IP Node Type.
                                      # vedi
                                      #http://www.networksorcery.com/enp/protocol/bootp/options.htm
# dhcp-host=00:13:8f:c2:bc:eb,ignore  # non fornisce alcun indirizzo ip alla
                                      # nic identificata
                                      # dal mac address 00:13:8f:c2:bc:eb
# dhcp-host=00:13:8f:c2:bc:eb,p41500,10.0.0.55,30m    # assegna alla nic
                                                      # identificata dal
                                                      # mac address
                                                      # 00:13:8f:c2:bc:eb
```

```
                                                        # l'indirizzo ip
                                                        # 10.0.0.55,
                                                        # assegna anche il
                                                        # nome host
                                                        # p41500 e
                                                        # specifica come
                                                        # tempo di lease
                                                        # 30 minuti
dhcp-leasefile=/etc/dnsmasq.d/lease       # file che registra gli ip erogati.
```

Ora un esempio un poco piu' elaborato, ove un pc con slackware 14.2 eroga il servizio di condivisione internet (nat) , servizio dhcp e servizio dns , su due reti distinte. La linux box in oggetto ha il seguente indirizzamento:

```
eth0 = 192.168.25.1 , da questo indirizzo si raggiunge internet
eth1 = 192.168.0.1   , questo indirizzo e' il default gw della rete
                       192.168.0.0/24
eth2 = 10.1.1.1        , questo indirizzo e' il default gw della rete
                       10.0.0.0/24
```

La condivisione internet viene fornita da iptables, tramite le seguenti direttive

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

iptables -A FORWARD -s 192.168.0.0/24 -j ACCEPT
iptables -A FORWARD -d 192.168.0.0/24 -j ACCEPT

 # eseguiamo il nat per la seconda rete
iptables -A FORWARD -s 10.1.1.0/24 -j ACCEPT
iptables -A FORWARD -d 10.1.1.0/24 -j ACCEPT
```

Ho inserite le direttive di iptables nel file /etc/rc.d/rc.local, ma sarebbe piu' corretto creare uno script di avvio, come insegna Volkerding.
Dnsmasq deve ora essere configurato per erogare i servizi su due distinte schede di rete. Ecco una possibile configurazione:

```
# per ottenere la lista completa delle opzioni
# digitare dnsmasq --help dhcp
# Opzioni DHCP
# 1- subnet mask
# 3- default gateway
# 6- dns server
# 28- broadcast address
# 44- wins server
# 46- netbios node type


        # niente cache per le risoluzoni negative
no-negcache

        # non usiamo /etc/resolv.conf
```

```
no-resolv

        # aggiunge sempre il nome di dominio
        #a al nome host
expand-hosts

        # nome del dominio
domain=veronese.lan

        # un poco di sicurezza , eliminiamo i
        #reverse-lookup
bogus-priv

        # indichiamo su quale nic (indirizzo) rimanere
        # in ascolto ed eorgare i servizi
listen-address=192.168.0.1
listen-address=10.1.1.1

        # indichiamo il range di indirizzi
        #  da erogare
dhcp-range=eth1,192.168.0.10,192.168.0.20,255.255.255.0,8h
dhcp-range=eth2,10.1.1.100,10.1.1.120,8h

        # indichiamo il gateway
dhcp-option=eth1,3,192.168.0.1
dhcp-option=eth2,3,10.1.1.1

        # indichiamo la netmask
dhcp-option=eth1,1,255.255.255.0
dhcp-option=eth2,1,255.255.255.0

        # indichiamo il dns da passare
        # ai client
dhcp-option=eth1,6,192.168.0.1
dhcp-option=eth2,6,10.1.1.1

        # indichiamo quali dns esterni usare
server=1.1.1.1

        # indichiamo il file di lease
dhcp-leasefile=/etc/dnsmasq.d/leases

        # abilitiamo i log
log-queries
log-dhcp
log-facility=/var/log/dnsmasq.log

        # aumentiamo un poco la sicurezza del tutto
domain-needed
bogus-priv

        # non leggiamo resolv.con
```

```
no-resolv

        # non ascoltiamo sull'interfaccia di
        # loopback
except-interface=lo
```

Per la stesura del presente ho consultato anche i seguenti link:

http://www.zaffa.org/2007/06/08/ubuntu-ltsp-thin-client-per-piccola-azienda-2/

http://iclame.scuole.bo.it/debian-scuolan/cap9.htm

http://wiki.archlinux.org/index.php/ArchSBS_-_DNS_dinamico_e_DHCP

http://infofreeflow.noblogs.org/index.phpop=printView&articleId=114715&blogId=1944

http://infocom.uniroma1.it/alef/cisterna/esercitazioni/dns.html

http://www.networksorcery.com/enp/protocol/bootp/options.htm

http://blogs.techrepublic.com.com/opensource/?p=293

http://ubuntrucchi.wordpress.com/2008/05/31/velocizzare-le-navigazione-con-una-cache-dns/

https://www.linux.com/topic/networking/advanced-dnsmasq-tips-and-tricks/

https://www.linux.com/training-tutorials/dnsmasq-easy-lan-name-services/

Inoltre all'interno della propria distribuzione nel path /usr/share/doc vi sono notizie ed esempi di configurazione.

Autore: Veronese Claudio, claudiovero@claudiove.com