DNS és DHCP szerver készítése egyszerűen: dnsmasq

1. sudo -s
2. apt-get install dnsmasq
3. **Beállítások helye:**
    a. vi /etc/dnsmasq.conf
        i. Itt jó példákat találsz
    b. vi /etc/default/dnsmasq
        i. Tudsz saját configot csinálni:
            1. CONFIG_DIR=/etc/dnsmasq.d
4. **Alap DNS beállítások**
    a. Saját beállítások külön fájlba, így a frissítés nem írja felül. Induljunk el pár alapvető DNS beállítással:
        i. vi /etc/dnsmasq.d/local.conf
            1. domain-needed
                a. Soha ne továbbítson DNS kérést, ha nincs domain része (nyilván helyi gépet keresünk)
            2. bogus-priv
                a. A privát tartományok (192.168, 172.16-31, 10) feloldására vonatkozó kéréseket NE továbbítsa
            3. local=/linuxakademia.lan/
                a. A helyi (belső hálózat) tartományát definiálja.
                b. Lehet több is (külön sorban ismételve).
                c. Ebben a tartományban a kéréseket nem továbbítja.
            4. interface=eth1
                a. Csak az eth1 csatolón szolgálunk ki (mindenre érvényes)
                b. A lo csatolót automatikusan hozzáadja.
                c. Vagy csinálhatod fordítva:
                    i. except-interface=eth0
                        1. Az eth0 kivételével minden csatolón kiszolgál (kevésbé bolond biztos).
                d. Esetleg IP címen figyeljen (alias csatolón (eth1:1) csak így megy)
                    i. listen-address=192.168.200.1
            5. domain=linuxakademia.lan
                a. A nem FQDN kéréseket kiegészíti, így a csak hostneves kéréseket is jól szolgálja ki.
            6. expand-hosts
                a. A /etc/hosts fájlban lévő rövid neveket is kiegészíti a domain-el
        ii. Nézzük meg így mit csinál!
            1. service dnsmasq restart
            2. cat /etc/resolv.conf
                a. A resolv.conf tartalmát lecseréli, így a helyi feloldás is a dnsmasq-n megy
                b. Honnan veszi a külső címeket? resolvconf
                    i. cat /etc/resolvconf/interface-order
                    ii. cat /etc/network/interfaces
                        1. dns-nameservers 192.168.2.1
                        2. De a DHCP kliens is beteszi a DNS-t
                    iii. ls -lh /var/run/resolvconf/interface/
                    iv. cat /var/run/resolvconf/interface/eth0.inet
                    v. cat /var/run/resolvconf/interface/lo.dnsmasq
                        1. Ez bírálja felül az eth0-tól jövőt (lásd interface-order)
            3. host 192.168.200.1
            4. host 192.168.200.10
            5. host desktop
            6. Honnan szedi?

a. cat /etc/hosts
b. Letiltása
i. no-hosts

5. **Alap DHCP beállítások**
   a. A DHCP szerver funkciót letiltja az adott csatolón
      i. #no-dhcp-interface=eth0
         1. Nincs értelme, ha az interfaces=eth1 benne van.
   b. Faék egyszerűségű DHCP szerver beűllítás
      i. dhcp-range=192.168.200.100,192.168.200.199,255.255.255.0,12h
         1. A 192.168.200.100 - 199 tartományban 12 órás bérleti idővel
   c. Éles üzem bekapcsolása. Nélküle minden kérésnél vár, hátha valaki más válaszol (nehogy felülbíráljon egy éles szervert)
      i. dhcp-authoritative
   d. Ha van tűzfal, akkor a bootpc -> bootps kéréseket engedélyezni kell:
      i. vi /etc/network/iptables.up.rules
         1. -A INPUT -m state --state INVALID -j DROP sor mögé:
         2. -A INPUT -i eth1 -p udp --sport bootpc --dport bootps -j ACCEPT
      ii. iptables-apply
   e. TESZT:
      i. service dnsmasq restart
      ii. tail /var/log/syslog
      iii. Desktopon DHCP-re váltás
      iv. Mi lett a cím?
         1. 192.168.200.182
         2. Nem a megszokott 192.168.200.10
         3. Arról később, hogyan lehet fix címet osztani.
         4. SSH bontás, visszalépés, sudo -s
         5. tail /var/log/syslog
            a. Megpróbálta a DNS-be is bejegyezni, de mivel már volt “desktop” a /etc/hosts-ban, nem ment.

6. **Extra DNS beállítások**
   a. Saját zónafájl használata a /etc/hosts mellett:
      i. addn-hosts=/etc/hosts.linuxakademia
      ii. seq 1 254 | awk '{ print("192.168.200."$1"\tdhcp-"$1".linuxakademia.lan\tdhcp-"$1) }' > /etc/hosts.linuxakademia
         1. A fájlból kitöröljük a már felvetteket + a hosts fájlból átmásoljuk ezeket (kivéve saját maga)
   b. Az adott domain feloldását a megadott IP című DNS szerver felé továbbítja.
      i. Pl: Van egy AD DC, ami kiszolgálja a linuxakademia.lan tartományt. Nyilván ilyenkor a saját beállításokban nincs domain=/linuxakademia.lan/. Az AD DC a 192.168.200.2.
      ii. #server=/linuxakademia.lan/192.168.200.2
      iii. #server=/200.168.192.in-addr.arpa/192.168.200.2
   c. Egy konkrét névhez tartozó cím felülbírálása:
      i. address=/facebook.com/127.0.0.1
         1. Előtte:
            a. host facebook.com
         2. service dnsmasq restart
         3. Utána:
            a. host facebook.com
      ii. address=/mail.linuxakademia.hu/192.168.200.4
         1. Pl. ugyan azon a néven érjük el a levelezést kintről és bentről, de bentről a belső IP-t adja
   d. Ha több csatolón/címen szolgál ki a dnsmasq, lehetőséged van beállítani, hogy egy adott címnek csak az ő tartományába eső címet adja vissza (ha van ilyen) a /etc/hosts fájlban felsorolt több címből:

i. localise-queries

e. Privát címek blokkolása (és naplózása), melyeket külső (upstream) DNS szerverek adnak vissza.
   i. stop-dns-rebind
   ii. rebind-localhost-ok
      1. A 127.0.0.0/8 az OK, ilyet néha adnak vissza legálisan is DNS szerverek (pl. black hole serverek)
   iii. #rebind-domain-ok=/zentyal.lan/slapic.lan/
   iv. TESZT
      1. service dnsmasq restart
      2. host gw.slapic.lan
         a. nem ad vissza címet
      3. tail /var/log/syslog
      4. vi /etc/dnsmasq.d/local.conf
         a. rebind-domain-ok=/zentyal.lan/slapic.lan/
      5. service dnsmasq restart
      6. host gw.slapic.lan
         a. Visszakapom a címet.

7. Extra DHCP beállítások

a. Fix IP beállítása
   i. #dhcp-host=00:0c:29:29:bc:6a,192.168.200.10
   ii. A /etc/ethers fájlba is írhatod a MAC/IP párokat
      1. #read-ethers
         a. vi /etc/ethers
            i. 00:0c:29:29:bc:6a 192.168.200.10
   iii. Ha a gép ad a DHCP kérésben hostnevet:
      1. #dhcp-host=id:desktop,192.168.200.10
   iv. Ha pedig a gép neve és IP címe benne van a /etc/hosts fájlban:
      1. dhcp-host=desktop
   v. TESZT
      1. service dnsmasq restart
      2. Desktopon új cím kérése
   vi. Csak statikus címek osztása (nincs dinamikus):
      1. #dhcp-range=192.168.200.0,static
         a. Értelem szerűen kekk ethers vagy dhcp-host sorok.
   vii. Ugyan azt az IP címet adja mindkét MAC-nek (feltételezzük, hogy sosem lesznek egyszerre elérhetőek):
      1. dhcp-host=11:22:33:44:55:66,12:34:56:78:90:12,192.168.200.60

b. IP cím kiosztás tiltása adott MAC-nek:
   i. #dhcp-host=11:22:33:44:55:66,ignore

c. Alapértelmezett átjáró megadása:
   i. #dhcp-option=3,192.168.200.1
      1. Nélküle a dnsmasq-t futtató gépnél a megfelelő csatoló első címét adja. Ez többnyire jó.

d. Másik DNS szerver megadása, ha nem a dnsmasq szologálja ki a munkaállomásokat:
   i. #dhcp-option=6,192.168.200.2
      1. Pl. a 192.168.200.2 egy AD DC DNS szervere

e. NTP szerver megadása:
   i. dhcp-option=42,0.0.0.0
   ii. dhcp-option=option:ntp-server,0.0.0.0
      1. A 0.0.0.0 azt jelenti, hogy a dnsmasq-t futtató gép címét adja.

f. WINS szerver megadása:
   i. dhcp-option=44,192.168.200.2
      1. Feltételezve, hogy a 192.168.200.2 futtat pl. egy Samba szervert.

g. WINS broadcast letiltása:
   i. dhcp-option=46,8

1. 1: broadcast
2. 2: csak WINS, nincs broadcast
3. 4: előbb broadcast, aztán WINS
4. 8: előbb WINS, aztán broadcast

ii. Egyéb NetBIOS jellemzők:

1. http://en.wikipedia.org/wiki/NetBIOS

h. Egyéb DHCP opciók

i. http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

8. Egyéb tippek és trükkök

a. Tűzfalon lehet növelni a biztonságot:

i. bind-interfaces

1. Meglévő csatolókon figyel, nem fut root jogokkal és nem tartja meg a CAP_NET_BIND képességet (nem is tud más csatolóra átmenni emiatt)

b. Ha ugyan ezen a gépen akarsz másik DNS szervert (pl. a dnsmasq a Samba4-el fut egy gépen és csak DHCP funkciót akarsz), a DNS nem tiltható le így a portot tudod átírni:

i. port=5353

c. Hol vannak a kiosztott címek?

i. cat /var/lib/misc/dnsmasq.leases

d. Levelező szerver beállítás (MX)

i. mx-host=linuxakademia.lan,mail.linuxakademia.lan,10

1. A linuxakademia.lan levelező szervere a mail.linuxakademia.hu 10-es prioritással

ii. mx-target=mail.linuxakademia.lan

iii. localmx

1. A fenti kettő együtt: minden belső géphez a megadott név az MX
2. host -t mx linuxakademia.lan

iv. selfmx

1. A fentiek helyett: minden gép MX-e a dnsmasq-t futtató gép maga.

e. SRV rekord

i. srv-host=_ldap._tcp,server.linuxakademia.lan,389

1. host -t srv _ldap._tcp.linuxakademia.lan

f. TXT rekord

i. txt-record=linuxakademia.hu,"v=spf1 mx -all"

1. host -t TXT linuxakademia.hu