DHCP a DNS a jak se dají využít v domácí síti

Úvod

- síťové protokoly
- spolupodílí se na fungování Internetu

Opáčko o internetu

- „Síť sítí“ - menší sítě pospojované dohromady
- IP adresa – číslo, které identifikuje počítač v rámci sítě
  - veřejná – unikátní v celém Internetu
  - privátní – unikátní v rámci jedné sítě. Pro spojení v rámci internetu je závislá na NAT nebo proxy.
- Jednotlivé sítě jsou propojené pomocí směrovačů

DHCP

- Dodává klientům informace o síti
  - základní (IP adresa, nejbližší směrovač, DNS servery)
  - další (např. potřebné informace pro boot bezdiskových klientů ze sítě
- Rozšiřuje starší protokol BOOTP
- Navrženo původně pro správu rozsáhlých sítí

Vlastnosti DHCP

- IP adresy přiděluje na určitou dobu
- Rozšiřitelnost – protokol dnes může přenášet informace, s kterými se v původním návrhu nepočítalo
- Rozšířenost - „každý systém si umí nakonfigurovat síť podle DHCP“
- Málo zatěžuje síť svým provozem
- Správce má síť pod kontrolou

DHCP - přidělování adres

- doba zápůjček
- změna adres

Programy pro práci s DHCP

- Servery
  - ISC (`dhcpd`)
  - Microsoft
  - „Hardwarové routery“
- Klienti
  - ISC (`dhclient`)
  - Microsoft
  - `dhcpcd`
  - RedHat (`pump`)

Kde se nepoužívá

- Pouze v malých sítích bez cestujících notebooků – všude jinde je výhodnější jej použít.

DNS

- „Služba doménových jmen“
- Překládá jména (linuxvbrne.org) na IP adresy a naopak

Vlastnosti DNS

- Volá se na začátku naprosté většiny spojení
- distribuovaná hierarchická databáze: `www.linuxvbrne.org.` `z.x.y.w.in-addr.arpa.`

Programy pro DNS

- servery
  - BIND (Berkeley Internet Name Domain; ISC)
  - Microsoft
  - tinydns (D. J. Bernstein)
- resolver
  - libc

Kde se používá

- všude :-)

Konec první části

DHCP a DNS v malé síti

Kdy je vhodné nasadit doma DHCP

- notebook pohybující v různých sítích
- více než 4 počítače v síti

Kdy se vyplatí nasadit doma DNS server

- připojení s dlouhými odezvami
- častá přetížení jmenných serverů ISP
- možnost adresovat počítače s adresami přidělenými DHCP serverem

Mé požadavky na tyto servery

- DHCP server musí pro různé OS přidělit IP adresy z různých rozsahů
- Jednotlivé počítače musí být dostupné pod svými jmény
- Rozšiřitelnost v případě propojení s dalšími lidmi v domě

Řešení

- Starý počítač
  - Pentium 133, 64MiB RAM
  - 2 disky v RAID 1
  - Debian Sarge
- `dhcpd`
  - `option dhcp-client-identifier`
- BIND
  - dynamické aktualizace DNS

Počítač

- adresáře dhcpd:
  `/etc/dhcp3`
  `/var/lib/dhcp3`
- adresáře BINDu
  `/etc/bind`
  `/var/cache/bind`

Nastavení dhcpd

- Rozdělení klientů do tříd
  - známý identifikátor
  - (známá MAC)
  - ostatní
- nastavení sítě a podsítí
- nastavení jmen pro klienty
- Společný tajný klíč s BINDem

Příklad /etc/dhcp3/dhcpd.conf

- include *soubor_s_tajnym_klicem;*
  ddns-update-style interim;
  deny clinent-updates;
  ddns-domainname "dum";
  ddns-rev-domainname "168.192.in-addr.arpa";
  zone dum. {
  primary 192.168.1.1;
  key key.dum.;
  };
  zone 162.198.in-addr.arpa { … };
  class "unix" {
  match if (option dhcp-client-identifier = "*ID1*") or
  (option dhcp-client-identifier = "*ID2*");
  }
  option domain-name-servers 192.168.1.1,
  dalsi_dns_server;

/etc/dhcp3/dhcpd.conf – pokračování

- ```
  subnet 192.168.1.0 netmask 255.255.255.0 {
     authoritative;
     option subnet-mask 255.255.255.0;
     option routers     192.168.1.1;
     pool {
        range 192.168.1.2 192.168.1.126;
        allow members of "unix";
        deny unknown clients;
     };
     pool {
        range 192.168.1.129 192.168.1.254;
        allow unknown clients;
     };
  }
  host david {
     option dhcp-client-identifier "ID1";
     ddns-hostname "david";
  }
  ```
  ```

Sdílený klíč

- příkaz `dnssec-keygen`:
  `dnssec-keygen -a HMAC-MD5 -b 512 -n ZONE dum.`
  vytvoří dvojici souborů:
  `Kdum.+157+42627.{key|private}`
- *rozsypaný_čaj* ze souboru *.private:
  Private-key-format: v1.2
  Algorithm: 157 (HMAC_MD5)
  Key: *rozsypaný_čaj*
  zkopírovat do souboru *soubor_s_tajnym_klicem*:

```
key key.dum. {
   algorithm HMAC-MD5.SIG-ALG.REG.INT;
   secret    rozsypaný_čaj;
}
```

BIND na Debianu Sarge

- základ konfigurace (netřeba upravovat) `/etc/bind/named.conf`
- všeobecné volby `/etc/bind/named.conf.options`
- definice zón `/etc/bind/named.conf.local`
- zónové soubory /var/cache/bind

Příklad named.conf.options

- options {
    directory "/var/cache/bind";
    allow-query { 127/8; dalsi_rozsahy; };
    allow-transfer { none; };
    listen-on { 127.0.0.1; 192.168.1.1; };
    forward first;
    forwarders { *dns_server_ISP*; };
  };
  include "*soubor_s_klicem*";

Příklad named.conf.local

- zone "dum" {
    type master;
    file "/var/cache/bind/db.dum";
    allow-update { key key.dum. ; };
  }
  zone "168.192.in-addr.arpa" {
    type master;
    file "/var/cache/bind/db.192.168";
    allow-update { key key.dum. ; } ;
  };

Zónový soubor db.dum

```
$ORIGIN .
$TTL 604800     ; 1 week
dum             IN SOA  server.dum. root.server.dum. (
                        2005103164 ; serial
                        604800     ; refresh (1 week)
                        86400      ; retry (1 day)
                        2419200    ; expire (4 weeks)
                        604800     ; minimum (1 week)
                        )
                        NS      server.dum.
                        MX      10 mail.dum.
mail                    CNAME   server
server                  A       192.168.1.1
```

Zónový soubor db.192.168

```
$ORIGIN .
$TTL 604800     ; 1 week
168.192.in-addr.arpa. IN SOA 168.192.in-addr.arpa.
root.server.dum. (
                        2005103164 ; serial
                        604800     ; refresh (1 week)
                        86400      ; retry (1 day)
                        2419200    ; expire (4 weeks)
                        604800     ; minimum (1 week)
                        )
                        NS      server.dum.
1.1                     PTR    server.dum.
```