Linux jako broadband router (2)

Ondřej Caletka

O.Caletka@sh.cvut.cz
http://www.pslib.cz/caletka

Linux jako broadband router

- *Volíme adresní rozsah*
- *Síťování z příkazového řádku*
- *Konfigrace NATu*
- *DHCP server*
- **DNS server (forwarder)**
- **Provázání DHCP a DNS**
- **Tipy a triky**

Jak vlastně DNS funguje?

- pocitac.domena.cz**.**
- čte se zprava
- musíme znát servery obsluhující kořenovou doménu . - slabé místo Internetu
- seznam se získá z ftp://ftp.internic.net/domain/named.root
- postupným dotazováním až k cíli

DNS server - forwarder

- Má vlastní cache. Ušetří zatěžování linky DNS dotazy
- Nejrozšíření opět od ISC – BIND (named)
- Standardní konfigurace – odpovídá na dotazy prostřednictvím kořenových serverů
- Můžeme si zařídit vlastní interní doménu
- Konfiguruje se v /etc/named.conf

named.conf

```
options {
        directory "/var/bind";
        listen-on { 127.0.0.1; 192.168.9.1; };
        forwarders {
              147.32.127.240;
              147.32.80.9;
        };
        pid-file "/var/run/named/named.pid";
};
zone "doma.net." IN {
        type master;
        file "pri/doma.net.zone";
        allow-update { none; };
};

zone "9.168.192.in-addr.arpa" IN {
        type master;
        file "pri/9.168.192.zone";
        allow-update { none; };
};
```

Zónové soubory

- Definují jednotlivé zóny – domény
- Každá doména má dvě zóny
- Mohou být primární a sekundární
  - primární musíme vytvořit
  - sekundární se okopírují automaticky z primárního serveru (záložní DNS)
- Jsou umístěny obvykle v /var/named/{pri,sec} nebo /var/bind/{pri,sec}
- Obsahují Resource Records a Start Of Authority

Definice zón

- Obecný formát záznamů RR (Resource Record)
  - <name> [<ttl>] [<class>] <type> <data>
  - komp 3600 IN A 10.0.0.1
- Dva druhy zón
  - přímá – převádí jména na IP adresy
    - jméno A IP (kanonické jméno)
    - alias CNAME jméno (alias)
  - reverzní – převádí IP adresy na jména
    - IP PTR jméno (pointer)
- Na začátku každého souboru je SOA

Co je vlastně reverzní záznam?

- Záznam ve speciální doméně in-addr.arpa.
- Příklad: adresa 147.32.123.19 má reverzní záznam uložen v doméně 19.123.32.147.in-addr.arpa.
- Proč obráceně?
- Podobně fungují také např. enum záznamy enum.arpa. pro hledání VoIP telefonů

Příklad - doma.net.zone

```
@       IN      SOA     ns.doma.net. root.doma.net.   (
                                      2006100101 ; Serial
                                      28800      ; Refresh
                                      14400      ; Retry
                                      604800     ; Expire -
  1 week
                                      86400 )    ; Minimum
                IN      NS      192.168.9.1
                IN      A       192.168.9.1

localhost.      IN      A       127.0.0.1

k5              IN      A       192.168.9.1
server          IN      CNAME    k5
wpad            IN      CNAME    k5
evo             IN      A       192.168.9.2
```

Příklad - 9.168.192.zone

```
9.168.192.in-addr.arpa IN SOA  k5.doma.net. root.k5.doma.net. (
                                2006100101 ; serial
                                28800      ; refresh (8 hours)
                                14400      ; retry (4 hours)
                                3600000    ; expire (5 weeks 6
   days 16 hours)
                                86400      ; minimum (1 day)
                                )
                        NS      k5.doma.net.
1                       PTR     k5.doma.net.
2                       PTR     evo.doma.net.
```

Testování nameserveru

- Postaru
  - nslookup
- Ponovu
  - host <jméno|IP>
  - dig <jméno domény> <typ dotazu>
- Ukázka

Provázáni DHCP a DNS

- DHCP server přidělí dynamickou adresu
- Adresa se zapíše do lokální domény pod jménem, které počítač při DHCP dotazu předal

- Postup:
  1. Zkonfigurujeme BIND jako dynamický
  2. Naučíme se updatovat DNS záznamy Dynamicky
  3. Řekneme DHCP serveru, aby to dělal

Dynamický nameserver

- Lze přidávat záznamy za běhu a to i ze vzdáleného počítače.
- NELZE editovat zónové soubory ručně – vede si žurnál
- Generování klíče (symetrická šifra):
  - dnssec-keygen -a HMAC-MD5 -b 64 -n USER dhcp_k
  - vytvoří dva soubory s (identickými) klíči
  - soubor .private si schováme pro ruční update

Úprava souboru named.conf

```
options {...};
key "dhcp_k" {
     algorithm "HMAC-MD5";
     secret "xxxxxxxx";
}
zone "doma.net." IN {
        type master;
        file "pri/k5.zone";
        allow-update { key "dhcp_k"; };
};

zone "9.168.192.in-addr.arpa" IN {
        type master;
        file "pri/9.168.192.zone";
        allow-update { key "dhcp_k"; };
};
```

Test – ruční update DNS

- K zasahování do DNS slouží utilita *nsupdate*, které se jako parametr předá soubor s klíčem:
  - nsupdate -k klic.private
- Program pracuje interaktivně, činnosti provádí po příkazu *send*, nebo po prázdném řádku
- Základní syntax:
  - zone doma.net.
  - update <add|delete> <RR>
- RR vždy musí obsahovat TTL
- Např: *update add komp.doma.net. 3600 A 10.0.0.1*

Úprava konfigurace dhcpd.conf

```
key dhcp_k {
        algorithm HMAC-MD5;
        secret "xxxxxxxxx";
}
zone doma.net. {
        primary 127.0.0.1;
        key dhcp_k;
}
zone 9.168.192.in-addr.arpa. {
        primary 127.0.0.1;
        key dhcp_k;
}
```

Závěr DNS

- Pěkný návod o síťování v linuxu na
  http://www.pslib.cz/ke/manuals/linux/network/index.phtml
  http://www.pslib.cz/ke/manuals/linux/pripojeni
- O (statické) DNS je hodně v LDP:
  http://knihy.cpress.cz/DataFiles/Book/00000675/Download/K0819.pdf
- Seriál na rootovi:
  http://www.root.cz/serialy/linux-jako-internetova-gateway/

Wana v Praze

T3 pod Ruskem

Tipy a triky

- HTTP proxy – cache server
- Automatická konfigurace MSIE a spol
- Captive portal
- SAMBA – tanec s okny
- NFS – tanec s UNIXy
- Diskuze

HTTP proxy - cache

- V dnešní době spíš přežitek, ale při vhodné konfiguraci může ušetřit opakované stahování update
- Jeden velice výkonný se jmenuje Squid
- Standardně cachuje pouze pro localhosta, ostatním píše Cache Access Denided
- Doladí se cca. uprostřed konfiguračního souboru

Transparentní proxy

- Použití proxy serveru s sebou nese nutnost konfigurace každého prohlížeče.
- Dá se to obejít přesměrováním požadavků na port 80 do squida
- Má to několik nevýhod (nemožnost autentifikace, zneužívání portu 80 ne-HTTP protokoly)

Automatická konfigurace MSIE...

- Prohlížeče si jsou schopni stáhnout konfigurační skript
- Standardně z adresy
  - http://wpad.domena.net/wpad.dat
- Proto je dobré, dát Web serveru alias wpad

Captive portal

- Řešení typu: eduroam-simple; Internet P5; kdysi ADSL dashboard
- Používá kouzlení s firewallem, arping pro zjišťování aktivity, RADIUS pro ověření
- Monolilická řešení s nesnadnou editací, přizpůsobením.
- Wikipedia; Google: Captive portal

Samba – Okolní počítače

- Umožňuje spolupráci s Windows
- Nedůležitější nastavení:
  - security=share … sdílené položky - Win98
  - security=user … autentifikace uživatele – WinNT
- Podpora českých názvů souborů
  - unix charset = ISO8859-2

NFS – Network File System

- Obdoba protokolu SMB mezi UNIXovými systémy
- Server nfsd pracuje na portu určeném službou portmap.
  - => Pro server portmap, nfsd; pro klienta portmap
- Konfigurace v /etc/exports
- Vzdáleně detekujeme pomocí *showmount --exports host*
- Tuhnutí systému -> *mount -o nolock host:/export...*

The End

It's time to turn off the light
This has been such a beautiful night
We have served you a lot of delights
And some really wonderful sights

My friend, this is the end
So long and see you soon again
Bye bye, kissing you hi
Someday we will be back together

Aqua – Goodbye to the Circus