
Desatero (až čtrnáctero) zavedení IPv6

1. Získat prefix
2. Zprovoznit routing k páteři a k serverům
3. Zprovoznit dual stack na infrastrukturních serverech (DNS, DHCP, monitorování)
4. Zprovoznit DNS přes IPv6 (případně DHCPv6)
5. Delegovat si reverzní doménu
6. Připravit adresní plán
7. Zprovoznit routing na páteřních sítích instituce (metropolitní, areálové, budovy)

Desatero

8. Zprovoznit veřejné Weby duálně
9. Nainstalovat Squid 3.1 (duální proxy), připravit `wpad.dat`
10. Spustit monitorování
11. Spustit RA klientům
12. Další služby (SSH, FTP, IMAP, POP, NTP, ...)
13. Mail (SMTP a publikovat MX)
14. Zvyšování propustnosti a redundance

Bod 1. Získat prefix

- V rámci Cesnet není problém, je k dispozici prefix 2001:718::/32, každá instituce dostává /48
- Většina má, kdo ne, požádá CESNET NIC, viz <http://www.cesnet.cz/nic/>
 - je k dispozici 65536 subnetů standardní délky /64
 - pro srovnání, standardní prefix IPv4 /16 při standardním dělení /24 má 256 subnetů, při dělení po /30 (spojky) má 16384 subnetů
 - není problém „plýtvat“ prefixy standardní délky 64
 - pokud za tím nejsou pádné důvody (a znalosti), nepoužívat pro sítě jinou délku prefixu než 64!
 - více viz bod 6 – Adresní plán

Bod 2. Dostat se na páteř Cesnet

- Směrovače páteřní sítě CESNET2 podporují protokoly IPv4 i IPv6 (dual stack)
- Obvykle se tedy IPv6 dostane dovnitř stejným spojem, jako IPv4
- Podmínky:
 - mít vlastní router(y) pro napojení sítě instituce
 - nezbytná koordinace (ne vše funguje jak má)
 - připravit topologii sítě instituce, adresní plán, směrování (OSPFv3)
 - pokud je instituce napojena na více směrovačů, pak BGP4
 - pro začátek stačí napojit VC, infrastrukturní servery
 - podrobněji viz <http://www.cesnet.cz/ipv6/pripojeni.html>

Bod 2. Dostat IPv6 k serverům

- Předpoklad: IPv6 se dostane k serverům stejnou sítí jako IPv4 (duální protokol v rámci jedné lokální sítě)
 - lze i jinak (zavést IPv6 VLAN), ale není to praktické a spíše to přinese problémy
 - pro L2 síť je jedno, jestli do ní směřujeme IPv6 nebo IPv4 (s výjimkou šíření multicastů)
 - zejména v počátku je obvyklé, že IPv6 router není fyzicky totéž zařízení jako IPv4 router – toky dat budou řádově nižší, lze vystačit s pomocným IPv6 routerem připojeným na páteřní switch jedním spojením
 - při upgradech je třeba počítat se sjednocením, jedna krabice by měla umět oboje, není to ale priorita při zavádění (nevymlouvat se, že to nejde bez \$\$\$)

Bod 3. Zprovoznit dual stack

- Všechny systémy dnes umí, je jen otázka konfigurace
 - u serverů (a většiny aktivních prvků) zásadně staticky konfigurovaná adresa (volba adresy viz adresní plán) a default router (viz bod 10)
 - vypnout autokonfigurace,
 - v systémech Windows explicitně zakázat používání tunelů 6to4, ISATAP a Teredo (přes registry).
 - v první fázi nepublikovat AAAA záznamy pod normálními doménovými jmény (buď subdoména host.**ipv6**.dom nebo přípona host**6**.dom)
 - ověřit funkci, začít monitorovat dostupnost spojení (stačí ping6)

Bod 4. Zprovoznit DNS

■ Bind 9.6, 9.7

□ upravit acl (pokud jsou, typicky u rekurzivních):

- `acl internal { 127.0.0.1/32; ::1; IPv4_sítě;
2001:718:XXX::/56; };`
- `allow-recursion { internal; }`
- `allow-query-cache { interna; }`
- `allow-transfer { IPv4 adresy sekundárů;
IPv6 adresy sekundárů; }`

□ povolit IPv6:

- `listen-on { IPv4; 127.0.0.1; };`
- `listen-on-v6 { ::1; IP6 serveru; };`

□ doplnit standardní zóny:

- `zone "0.ip6.arpa" { type master; notify no;
file "loc6.rev"; };`
- `zone "8.B.D.0.1.0.0.2.ip6.arpa" { type master;
notify no; file "empty.dom"; };`

■ ...

Bod 4. Zprovoznit DHCPv6

- Jediný způsob jak dostat IPv6 adresy DNS serverů IPv6-only klientům
- Vista, Win7 standardně, Linux podle distribuce, není ale problém doinstalovat balíček, MAC OS X nemá
- ISC DHCP-4.1 (samostatná konfigurace, nutno provozovat zvlášť DHCP a DHCPv6):

```
# DNS name servers
```

```
option dhcp6.name-servers  
    2001:718:802:809::93e5:92b,  
    2001:718:802:808::93e5:80c;
```

```
# pozor na Vista SP1 bug (bude fit, vutbr, cz)
```

```
option dhcp6.domain-search "fit.vutbr.cz";
```

```
option dhcp6.sntp-servers  
    2001:718:802:809::93e5:90b;
```


Bod 4. Zprovoznit DHCPv6

```
subnet6 2001:718:802:8b0::/64 {  
    allow unknown-clients;  
# pokud chceme přidělovat dynamické adresy  
klientům z DHCPv6:  
    range6 2001:718:802:8b0::1:0:0  
           2001:718:802:8b0:00ff:ffff:ffff:ffff;  
# statická adresa (pozor na DUID)  
host guta { host-identifier option dhcp6.client-  
id 00:01:00:01:00:30:48:00:06:30:86:46;  
    fixed-address6 2001:718:802:808::93e5:80b; }  
}
```

pozor na
u/g bity

■ DHCPv6 relay

- buď umí router
- pokud ne, stačí dovést všechny sítě přes VLANy a použít ISC dhcrelay:

```
/usr/local/sbin/dhcrelay -6 -l vlan1 -l vlan2 -u em0
```

Bod 5. Reverzní DNS

- Zajistit delegaci (Cesnet NIC)
- Zavést zónu (nezapomenout na sekundární NS)

```
zone "2.0.8.0.8.1.7.0.1.0.0.2.ip6.arpa" {  
    type master;  
    file "ip6-vut.rev";  
};
```

- Připravit zónu (nutný nástroj, jinak špatně):

```
@ IN SOA ...  
@ IN NS ...  
$ORIGIN 0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.0.  
      8.0.2.0.8.0.8.1.7.0.1.0.0.2.ip6.arpa.  
1.0 PTR ip6-boz.fit.vutbr.cz.  
$ORIGIN 9.0.5.e.3.9.0.0.0.0.0.0.0.0.9.0.  
      8.0.2.0.8.0.8.1.7.0.1.0.0.2.ip6.arpa.  
b.0 PTR guta6.fit.vutbr.cz.  
7.1 PTR www.fit.vutbr.cz.
```

Bod 5. Reverzní DNS

- Co do reverzních záznamů?
 - staticky přiřazené IPv6 adresy, tj. servery, aktivní prvky
- Temporary adresy a náhodné SLAAC adresy ručně nelze spravovat, jedině přes DDNS.
- Reverzní záznamy u klientů ztrácí s IPv6 použitelnost.