

Lokální DNS a DNSSEC

Datum zpracování: 21. 11. 2023

Zpracovali: Kohout Daniel, Knespl Daniel, Koten Tomáš, Musilová Anežka, Svobodný Hynek Václav



Zadání

Zapojte lokální síť s DHCP.

1. Nakonfigurujte router a připojené počítače tak, aby DNS počítačům v síti přiděloval jména s koncovkou **.lan**.
2. Příkazem **dig +dnssec** zkонтrolujte záznamy lokálních počítačů a serveru www.tul.cz
3. Porovnejte s výsledkem při zapojení přímo do sítě (s veřejnou adresou 147.230.x.x)
4. Do routeru v terminálovém připojení doinstalujte DNS **unbound** a nakonfigurujte předávání DNSSEC záznamů do sítě.
5. Doplňte **ubound** o IANA klíč umožňující ověřování lokálních DNSSEC záznamů.
6. V průběhu práce pořízujte screenshoty a záznamy použitých příkazů; použijte je v elaborátu a okomentujte postup.

Úlohu zpracovávejte ve 2 - 5členných týmech.

Elaborát zpracujte do šablony v záhlaví kruzu, odevzdávejte ve formátu PDF.

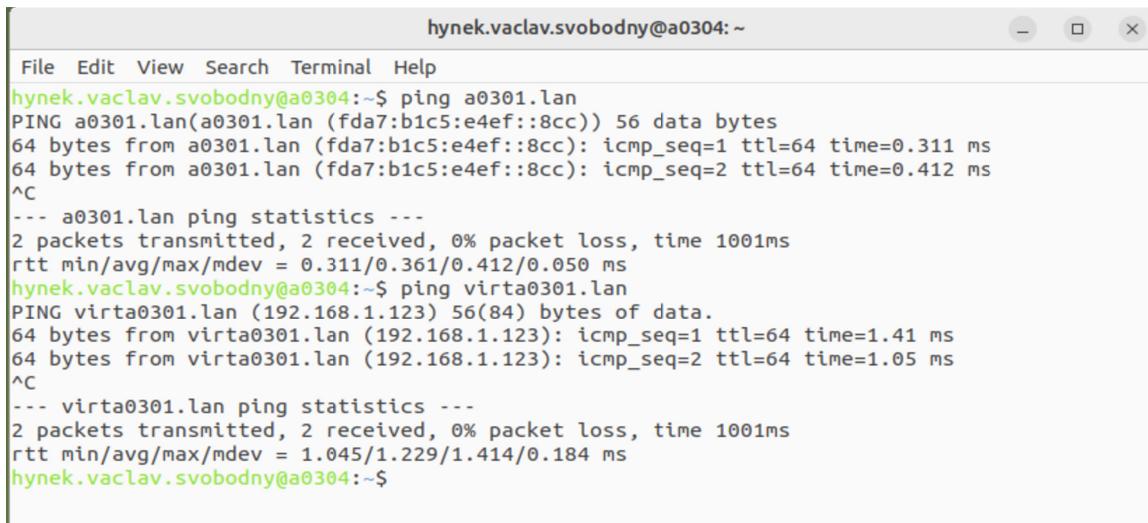
Do abecedně seřazeného seznamu řešitelů na úvodním listu uveďte reálné složení týmu!



Postup

1. Konfigurace routeru a připojených počítačů

- Ověření propojení zařízení v síti → **ping [domain name]**



```

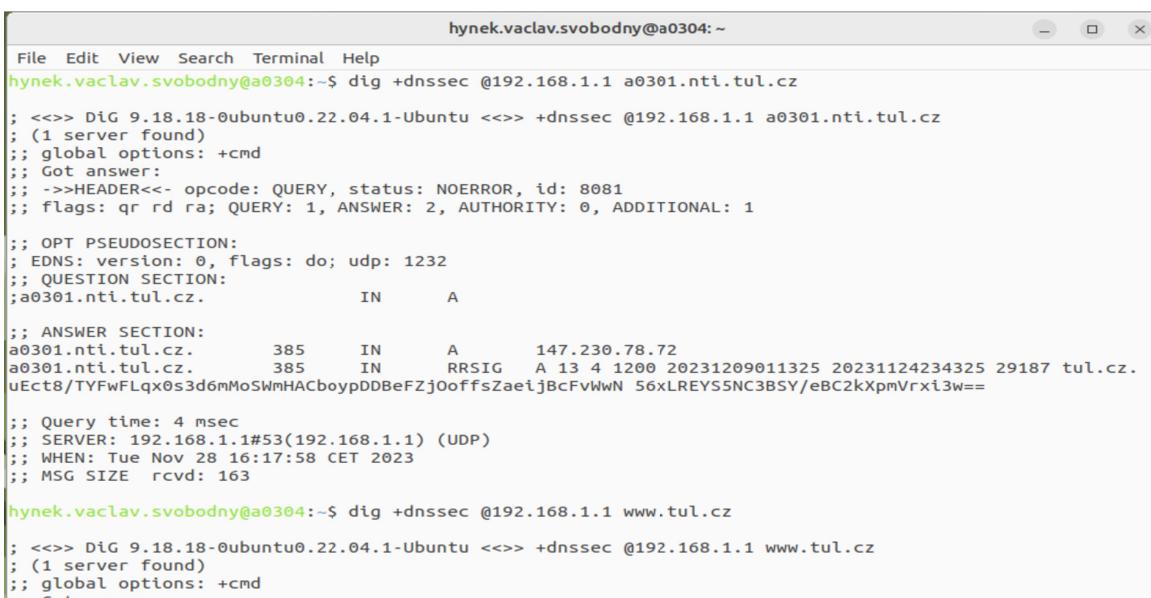
hynek.vaclav.svobodny@a0304:~$ ping a0301.lan
PING a0301.lan(a0301.lan (fda7:b1c5:e4ef::8cc)) 56 data bytes
64 bytes from a0301.lan (fda7:b1c5:e4ef::8cc): icmp_seq=1 ttl=64 time=0.311 ms
64 bytes from a0301.lan (fda7:b1c5:e4ef::8cc): icmp_seq=2 ttl=64 time=0.412 ms
^C
--- a0301.lan ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.311/0.361/0.412/0.050 ms
hynek.vaclav.svobodny@a0304:~$ ping virta0301.lan
PING virta0301.lan (192.168.1.123) 56(84) bytes of data.
64 bytes from virta0301.lan (192.168.1.123): icmp_seq=1 ttl=64 time=1.41 ms
64 bytes from virta0301.lan (192.168.1.123): icmp_seq=2 ttl=64 time=1.05 ms
^C
--- virta0301.lan ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.045/1.229/1.414/0.184 ms
hynek.vaclav.svobodny@a0304:~$
```

Obrázek 1: Příkaz ping

- Nastavení přidělování jména s koncovkou **.lan** bylo nastaveno implicitně.

2. Kontrola záznamů příkazem **dig +dnssec**

- Lokální počítače → **dig +dnssec @192.168.1.1 [domain name]**



```

hynek.vaclav.svobodny@a0304:~$ dig +dnssec @192.168.1.1 a0301.nti.tul.cz
; <>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <>> +dnssec @192.168.1.1 a0301.nti.tul.cz
; (1 server found)
; global options: +cmd
; Got answer:
; >>>HEADER<<- opcode: QUERY, status: NOERROR, id: 8081
; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; QUESTION SECTION:
;a0301.nti.tul.cz.           IN      A
;
; ANSWER SECTION:
a0301.nti.tul.cz.      385      IN      A      147.230.78.72
a0301.nti.tul.cz.      385      IN      RRSIG   A 13 4 1200 20231209011325 20231124234325 29187 tul.cz.
uEct8/TYFwFLqx0s3d6MmSwMhACboypDDBeFZjOoffsZaeijBcFvWwN 56xLREYS5NC3BSY/eBC2kXpmVrx13w==
;
; Query time: 4 msec
; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
; WHEN: Tue Nov 28 16:17:58 CET 2023
; MSG SIZE  rcvd: 163
hynek.vaclav.svobodny@a0304:~$ dig +dnssec @192.168.1.1 www.tul.cz
; <>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <>> +dnssec @192.168.1.1 www.tul.cz
; (1 server found)
; global options: +cmd
; Got answer:
```

Obrázek 2: Záznam lokálního počítače



- o server www.tul.cz → `dig +dnssec @192.168.1.1 www.tul.cz`

```

;; Query time: 4 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Tue Nov 28 16:17:58 CET 2023
;; MSG SIZE rcvd: 163

hynek.vaclav.svobodny@a0304:~$ dig +dnssec @192.168.1.1 www.tul.cz

; <>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <>> +dnssec @192.168.1.1 www.tul.cz
; (1 server found)
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1139
; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; QUESTION SECTION:
;www.tul.cz.           IN      A

;; ANSWER SECTION:
www.tul.cz.          1048    IN      CNAME    novy.tul.cz.
www.tul.cz.          1048    IN      RRSIG   CNAME 13 3 1200 20231209011325 20231124234325 29187 tul.
cz.ZVPC2Hv5Jqt61CqxjHP64cZzgAwpQVUUSgSoVar6KxAxu1/fq1ikWm6WU ujEWFXFhi/dzc5Q2XiYufZ53V0iayA==
novy.tul.cz.         1048    IN      A       147.230.18.195
novy.tul.cz.         1048    IN      RRSIG   A 13 3 1200 20231209011325 20231124234325 29187 tul.cz.
50m+KZj0p270tc4lAQHUSxwL7kv91yOKIIG7eWRSxMpC380VFIQZowHs mLvUJBjCHgrVGZHEGy2RUet9ykVxtQ==

;; Query time: 4 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Tue Nov 28 16:18:17 CET 2023
;; MSG SIZE rcvd: 278

```

Obrázek 3: Záznamy serveru www.tul.cz

- Výsledek při zapojení přímo do sítě (veřejná adresa 147.230.x.x)

- o Lokální počítače → `dig +dnssec [domain name]`

```

hynek.vaclav.svobodny@a0304:~
```

File Edit View Search Terminal Help
hynek.vaclav.svobodny@a0304:~\$ dig +dnssec a0301.nti.tul.cz

; <>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <>> +dnssec a0301.nti.tul.cz
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
; QUESTION SECTION:
;a0301.nti.tul.cz. IN A

;; ANSWER SECTION:
a0301.nti.tul.cz. 151 IN A 147.230.78.72

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Nov 28 16:19:53 CET 2023
;; MSG SIZE rcvd: 61

hynek.vaclav.svobodny@a0304:~\$ dig +dnssec www.tul.cz

; <>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <>> +dnssec www.tul.cz
; global options: +cmd
; Got answer:

Obrázek 4: Veřejný záznam lokálního počítače



- o server www.tul.cz → **dig +dnssec www.tul.cz**

```
;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Nov 28 16:19:53 CET 2023
;; MSG SIZE rcvd: 61

hynek.vaclav.svobodny@a0304:~$ dig +dnssec www.tul.cz

; <>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <>> +dnssec www.tul.cz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33908
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.tul.cz.           IN      A

;; ANSWER SECTION:
www.tul.cz.          249     IN      CNAME   novy.tul.cz.
novy.tul.cz.          249     IN      A       147.230.18.195

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Nov 28 16:19:58 CET 2023
;; MSG SIZE rcvd: 74
```

Obrázek 5: Veřejné záznamy serveru www.tul.cz

- o Při přístupu z veřejné adresy se v sekci ANSWER nezobrazí podpis DNSSEC

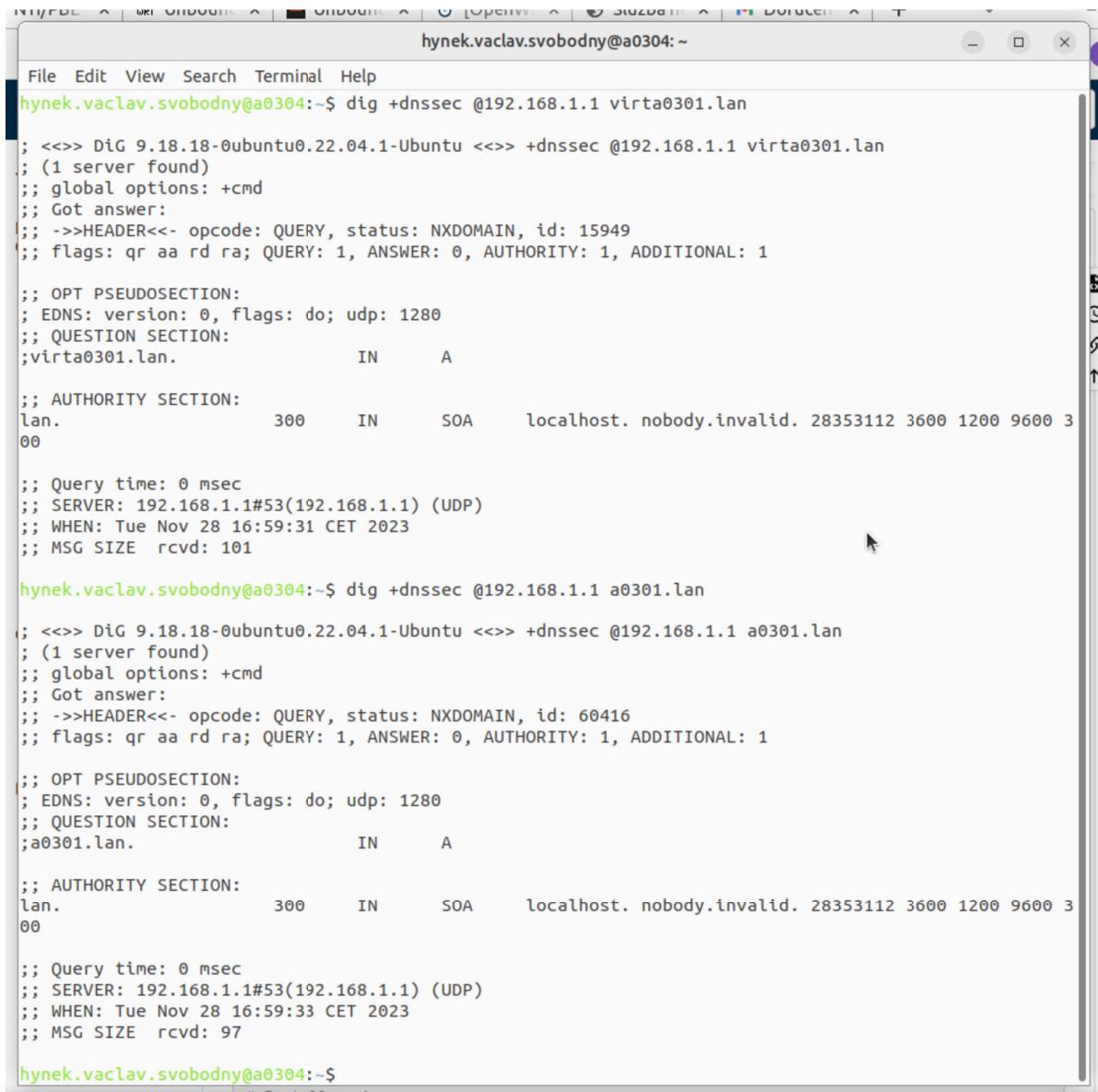
4. Instalace a nastavení **unbound**, aby podepisoval jména ***.lan**

- o Přihlášení do routeru příkazem **ssh root@192.168.1.1**
- o Aktualizace balíčkovacího systému → **opkg update**
- o Instalace DNS **unbound** → **opkg install unbound-daemon**
- o Konfigurace předávání DNSSEC záznamů do sítě → **uci set unbound.@unbound[0].validator="1"**
- o Aplikování změn → **uci commit unbound**
- o Pro jistotu jsme restartovali službu pomocí příkazu **service unbound restart**
- o Zastavení/nahrazení dnsmasq → **service dnsmasq stop**

```
root@a03r01:~# uci set unbound.@unbound[0].validator="1"
root@a03r01:~# uci commit unbound
root@a03r01:~# service unbound restart
unbound: default protocol configuration
unbound: default memory configuration
unbound: default recursion configuration
root@a03r01:~# service dnsmasq stop
root@a03r01:~#
```



- Test, že je **unbound** správně nastavený:



```
hynek.vaclav.svobodny@a0304:~$ dig +dnssec @192.168.1.1 virta0301.lan
; <>>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <>>> +dnssec @192.168.1.1 virta0301.lan
; (1 server found)
; global options: +cmd
; Got answer:
; ->>>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 15949
; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1280
; QUESTION SECTION:
;virta0301.lan.           IN      A
;
; AUTHORITY SECTION:
lan.                  300     IN      SOA      localhost. nobody.invalid. 28353112 3600 1200 9600 3
00
;
; Query time: 0 msec
; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
; WHEN: Tue Nov 28 16:59:31 CET 2023
; MSG SIZE  rcvd: 101

hynek.vaclav.svobodny@a0304:~$ dig +dnssec @192.168.1.1 a0301.lan
; <>>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <>>> +dnssec @192.168.1.1 a0301.lan
; (1 server found)
; global options: +cmd
; Got answer:
; ->>>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 60416
; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1280
; QUESTION SECTION:
;a0301.lan.           IN      A
;
; AUTHORITY SECTION:
lan.                  300     IN      SOA      localhost. nobody.invalid. 28353112 3600 1200 9600 3
00
;
; Query time: 0 msec
; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
; WHEN: Tue Nov 28 16:59:33 CET 2023
; MSG SIZE  rcvd: 97
```

Obrázek 6: Test DNSSEC



Závěr

Nejtěžší částí se ukázalo být započetí úlohy, jelikož se vyskytly problémy s nastavením DNS. Dále nás brzdilo pochopení zadání, ale pomocí častého dotazování jsem nakonec došli k požadovanému výsledku. Při této úloze jsme se trochu uskromnili a obsluhu terminálu jsme delegovali na jednoho člena týmu. Ostatní členové plnily funkce dohledávání informací, navádění, co dělat, psaní protokolu a poskytování psychické podpory.

