DNS, DHCP

Richard Biječek

Microsoft CERTIFIED IT Professional

Domain Name System

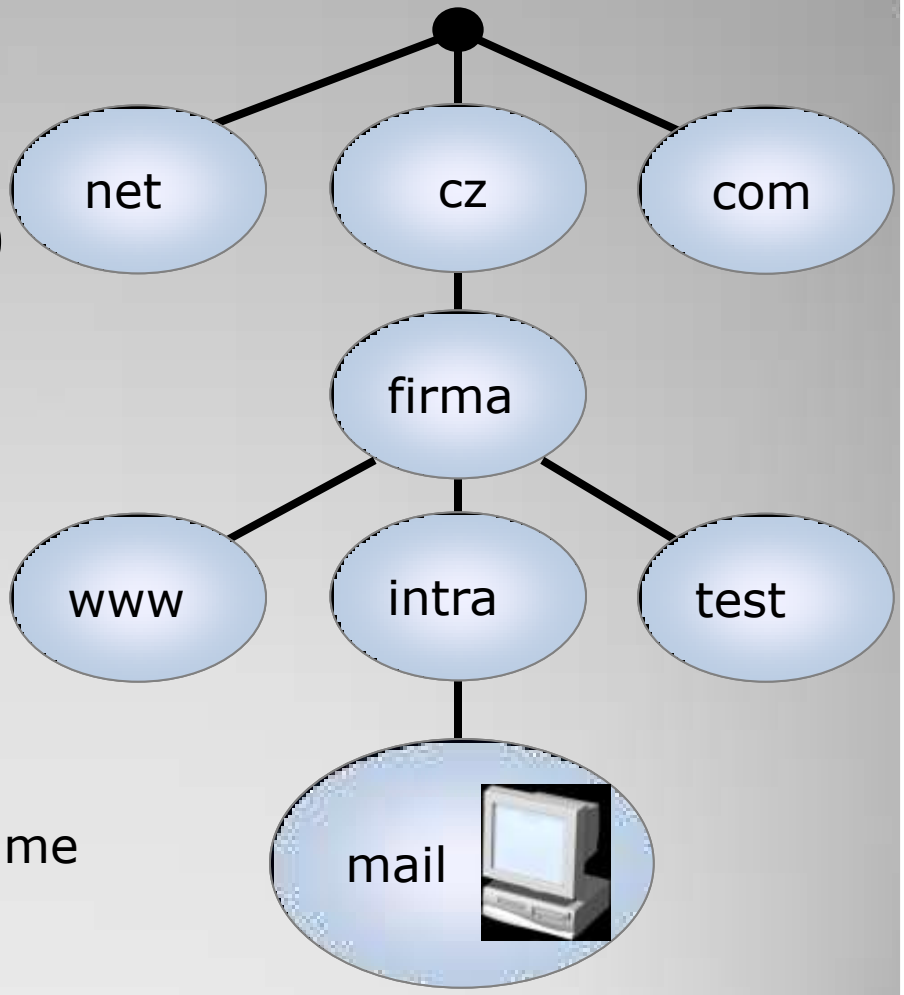
- DNS (Domain Name System)
  - Překlady názvů hostname
  - Informace o službách (např. mail servery)
  - Další služby (zpětné překlady, rozložení zátěže)
- Hlavní prvky DNS:
  - DNS server(y)
  - DNS klient(i)
  - DNS protokol
    - UDP 53, TCP 53

DNS infrastruktura

- Hierarchická distribuovaná databáze
  - Doménová jména (stromová struktura)
  - DNS zóny a jejich kopie (servery s daty)
  - Data v podobě záznamů různých typů
- DNS bylo navrženo pro potřeby internetu
- Prakticky nemá kapacitní omezení
  - Počet domén, záznamy, …

Domény, názvy

- Domény
  - Kořenová (root)
  - Top-level (1. úrovně)
  - 2. úrovně
  - …
- Název prostředku
  - Hostname
- Úplný název
  - FQDN:
    - Fully Qualified Domain Name



Domény, názvy

- Příklad:
  - Doména: *spo1045udom.local*
  - Hostname: *server01*
  - FQDN: *server01.spo1045udom.local*
- V internetu:
  - Doména: *seznam.cz*
  - Doména: *mail.google.com*
    - Samotná doména může reprezentovat prostředek
    - Rodělení FQDN na doménu a hostname není třeba

Podporované znaky

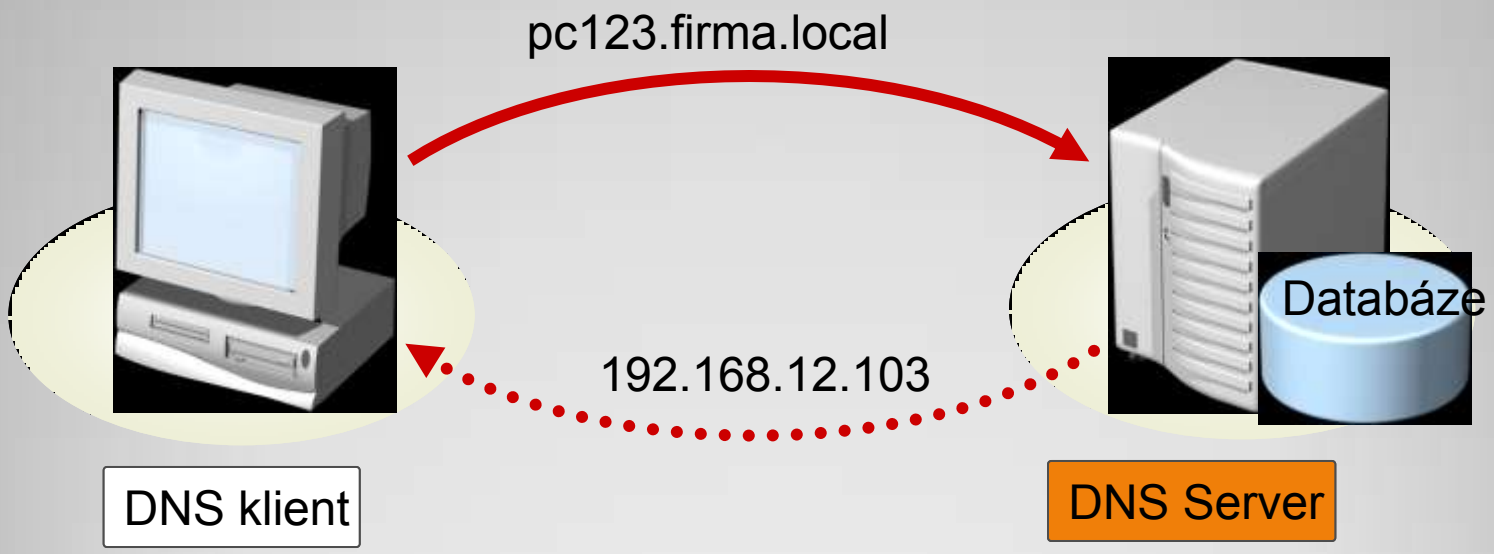
- 0 .. 9
- A .. Z
- a .. z (DNS není case sensitive)
- - (pomlčka)

- Použití jiných znaků záleží na implementaci serveru a klienta
- IDN v Internetu (háčkyčárky.cz)
  - non-ASCII znaky kódovány do ASCII

DNS komunikace

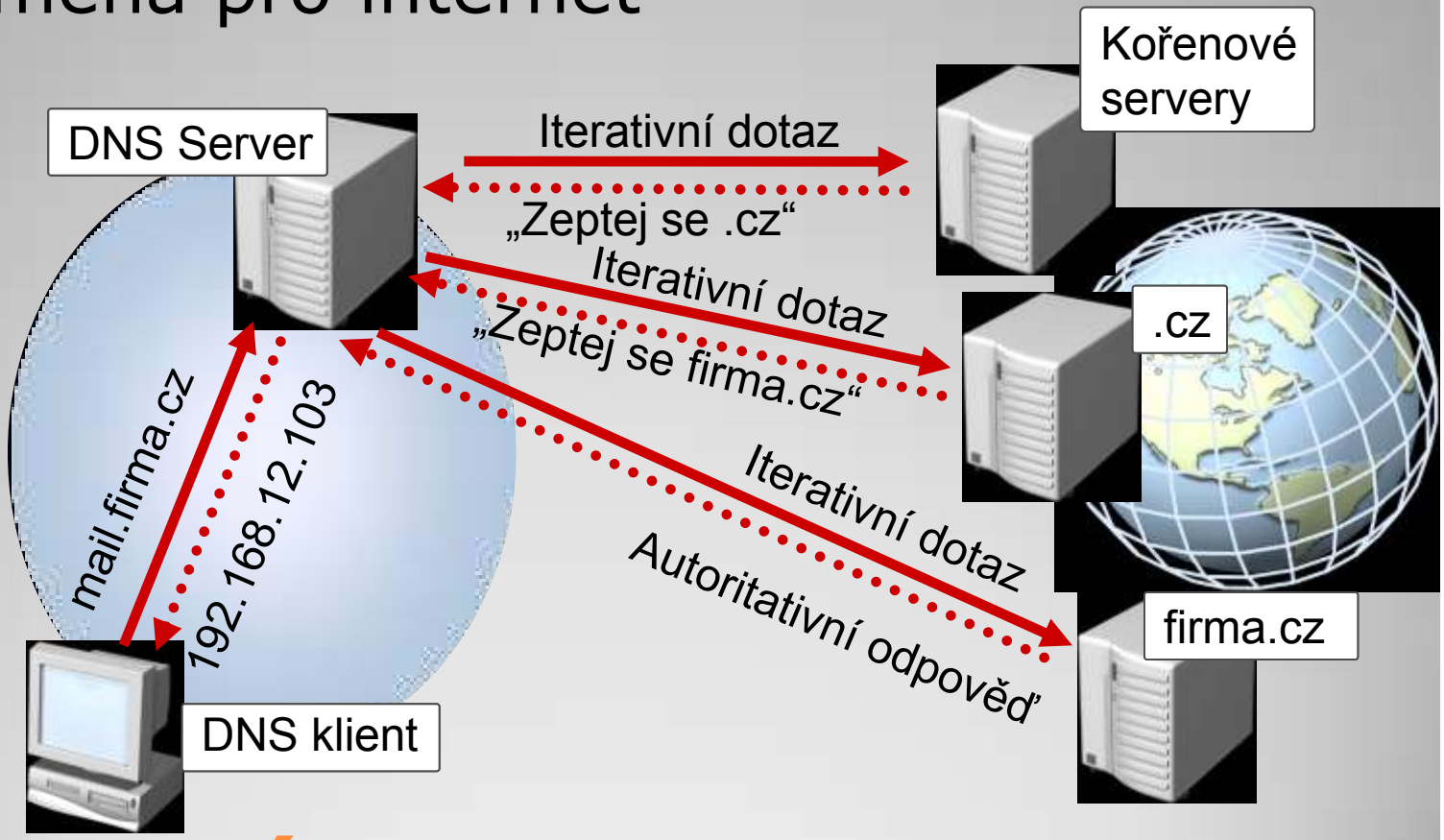
- Komunikace v DNS
- Klient – Server
- Server – Server
- Základem je DNS dotaz (DNS Query)
- Dotazy
  - Rekurzivní / Iterativní
- Odpověďi na dotazy
  - Autoritativní / Zprostředkované (neautoritativní)

- Klient se dotazuje (vždy rekurzivní)
- Očekává finální odpověď
  - = DNS server se může doptat dále (rekurze)



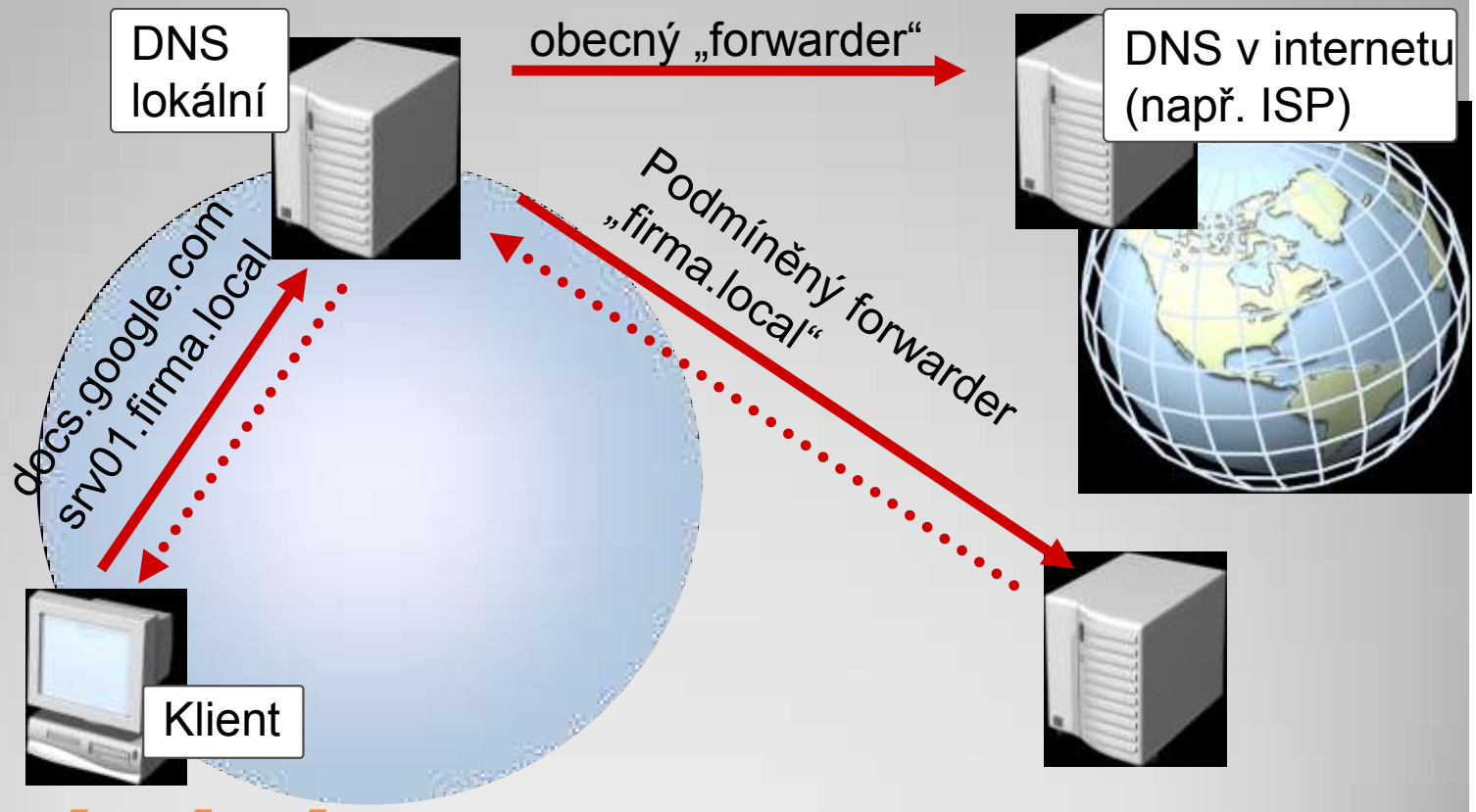
Rekurzivní dotaz

- Iterativní dotazy vytváří DNS servery
- Zejména pro internet



Iterativní dotaz

- DNS servery mohou předávat dotazy



Předávání dotazu

Předávání dotazu

- Při předávání (forwarding) vytváří DNS server rekurzivní dotaz
  - Chová se jako klient, očekává úplnou odpověď
- Dotazy do internetu
  - Předávání na server providera, apod.
- Dotazy na jiné vnitřní domény
  - Např. při kooperaci firem
  - V Internetu neexistují (xxx.local, xxx.intra)
  - Je nutno předat jinam, dle podmínky

DNS záznamy

- Data v DNS jsou tvořena záznamy
- Běžné typy záznamů:
  - **A** – IPv4 host; **AAAA** – IPv6 host
  - **CNAME** – alias
  - **MX** – mail exchanger
  - **SRV** – service locator
  - **PTR** – pointer (reverzní překlad)
  - **SOA** – start of authority
    - definuje některé parametry zóny
  - **NS** – name server

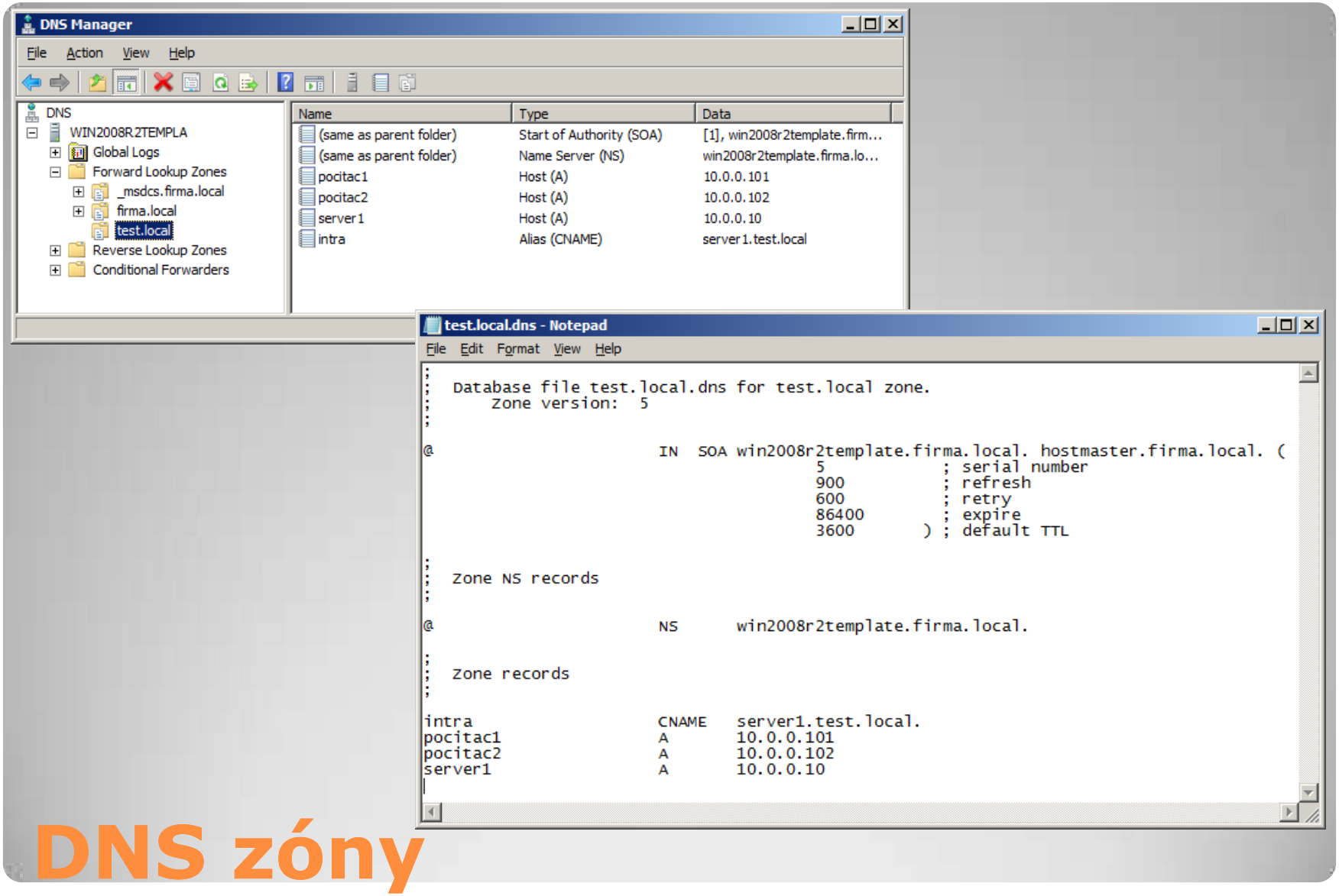
DNS zóny

- Kontinuální část DNS prostoru = zóna
- Zónu tvoří minimálně jedna doména
- Zóny dělíme na:
  - Obyčejné (data v textovém souboru)
  - AD Integrované (data v databázi AD)

  - Primární
  - Sekundární
  - Stub

DNS zóny

- Primární zóna
  - Zapisovatelná kopie DNS zóny
  - Každá zóna má právě jednu primární kopii
    - Neplatí pro AD-Integrované!!!, viz dále
- Sekundární zóna
  - Pouze pro čtení
  - Aktualizuje se tzv. „zone transfery“ z primární
  - Slouží pro redundanci a rozložení zátěže
  - V případě selhání primárního serveru lze „povýšit“ na primární


DNS Manager
File Action View Help
DNS
WIN2008R2TEMPLA
Global Logs
Forward Lookup Zones
_msdcs.firma.local
firma.local
test.local
Reverse Lookup Zones
Conditional Forwarders
Name Type Data
(same as parent folder) Start of Authority (SOA) [1], win2008r2template.firm...
(same as parent folder) Name Server (NS) win2008r2template.firma.lo...
pocitac1 Host (A) 10.0.0.101
pocitac2 Host (A) 10.0.0.102
server1 Host (A) 10.0.0.10
intra Alias (CNAME) server1.test.local
test.local.dns - Notepad
File Edit Format View Help
; Database file test.local.dns for test.local zone.
; Zone version: 5
@ IN SOA win2008r2template.firma.local. hostmaster.firma.local. (
5 ; serial number
900 ; refresh
600 ; retry
86400 ; expire
3600) ; default TTL
; Zone NS records
@ NS win2008r2template.firma.local.
; Zone records
intra CNAME server1.test.local.
pocitac1 A 10.0.0.101
pocitac2 A 10.0.0.102
server1 A 10.0.0.10

DNS zóny

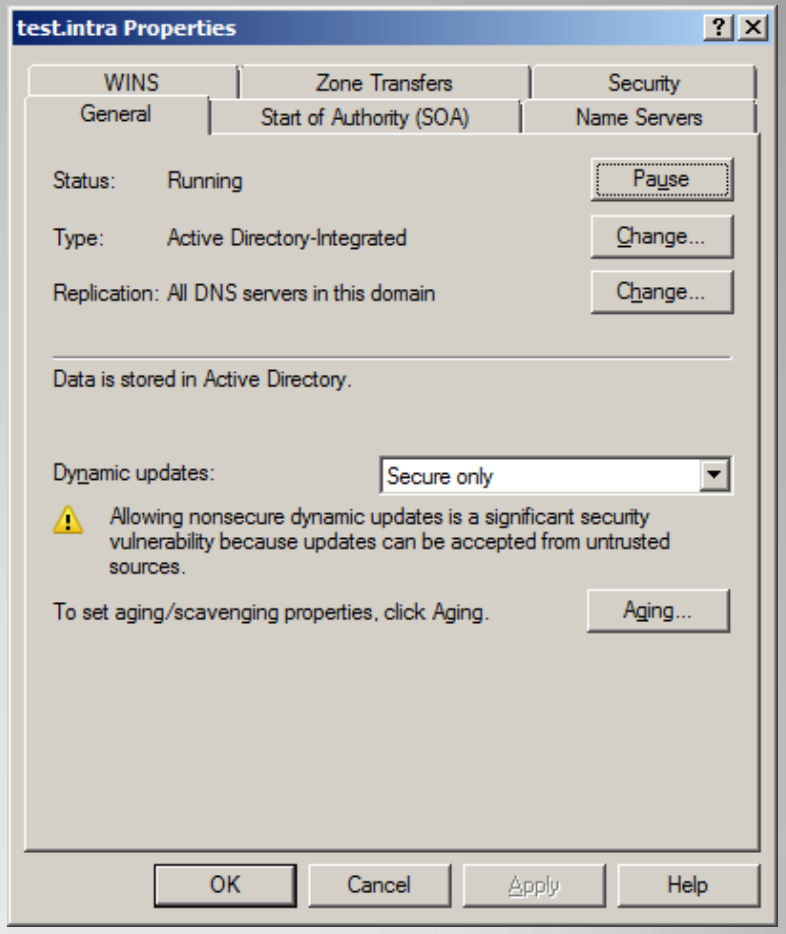
DNS zóny

- Obyčejné zóny – data v txt souborech
- C:\Windows\System32\DNS\zona.dns
- Kompatibilní formát souboru, dle RFC

AD integrované zóny

- AD Integrované zóny
- Data uložena v databází Active Directory
- Dostupné jen na doménových řadičích AD
- Výhody:
  - Může být více primárních kopií jedné zóny
  - Data mezi zónami přenáší replikace AD
  - Zabezpečené dynamické aktualizace (viz. dále)
- Nejsou k dispozici jako sekundární
  - Není pro to důvod

- Vlastnosti zóny



AD integrované zóny

Dynamické aktualizace

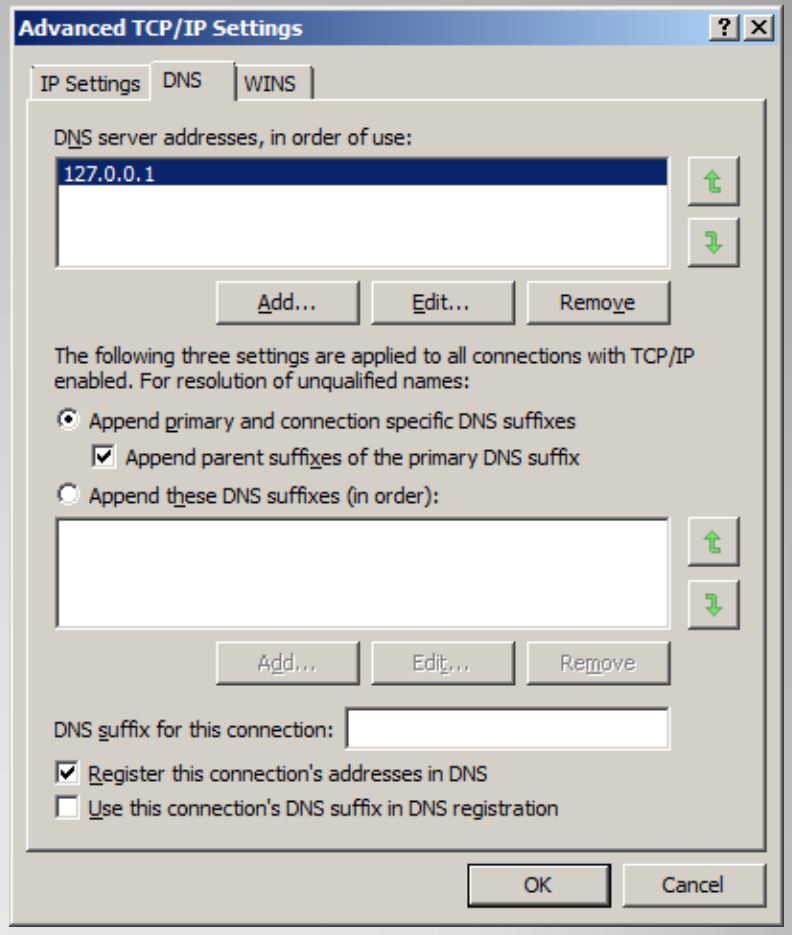
- DNS záznamy se netvoří jen ručně
  - Statické záznamy
- Je výhodné mít host záznam pro každý server i klienta
- Vzhledem k počtu ruční tvorba neúnosná
  - Dynamické záznamy
- Klienti provádí Dynamické registrace
  - Vytváří / aktualizují záznamy A (AAAA) a PTR

Dynamické aktualizace

- Ve spojení s AD integrovanými zónami
- Možnost zabezpečení
  - Zóna i její záznamy mají ACL (Security)
  - Zabrání vytvářet falešné záznamy
  - Klient musí být členem AD domény
- Pro rozlehlé domény
  - Vzdálené fyzické lokace jedné AD domény
  - Aktualizace probíhá na nejbližší DNS
  - U obyčejných zón zátěž WAN linky (problémy)

Nastavení DNS klienta

- Pořadí DNS serverů
- Překlad neúplných jmen
  - DNS dotaz je vždy na FQDN
- Automatické aktualizace (registarce)



Reverzní překlad

- Rozdělení zón z pohledu záznamů
  - Dopředné (všechny běžné – A, CNAME, MX, SRV, TXT, …)
  - Reverzní (PTR záznamy)
- Slouží zejména pro diagnostiku
- Na základě známe IP adresy vrací jméno
- Zóny nesou jména dle IP subnetů
  - „Jakoby naopak zapsané“ (priorita IP a DNS)

Užitečné nástroje

- DNS konzole
  - Plnohodnotný nástroj pro správu DNS serveru
- DNSCMD
  - Příkaz klasického příkazového řádku
  - Pro správu DNS serveru
- NSLOOKUP
  - Příkazová varianta DNS klienta, pro diagnostiku
- IPCONFIG /***DNS
  - Přepínače příkazu IPCONFIG, registrace, cache

DHCP

- Dynamic Host Configuration Protocol
- Služba DHCP Server
- DHCP klient
- Slouží k dynamické konfiguraci IP klienta
- Poskytuje nejen IP adresu
  - DNS servery
  - Výchozí bránu
  - WINS servery
  - Informace pro bootování ze sítě

DHCP konfigurace

- Nastavení DHCP pro subnet = „scope“
- Konfigurace se sestává z:
  - Rozsahu IP adres
  - Výjimek z rozsahu
  - Doby pronájmu
  - DHCP options

Doba pronájmu DHCP

- Server určí při poskytnutí konfigurace
- Klient může požádat o prodloužení
  - V 50% a v 87,5% uplnynulého času
- Po expiraci musí klient konfiguraci uvolnit
- Pro sítě bez pohybu klientů (pevné)
  - Velké hodnoty – hodiny až dny
- Pro např. wifi sítě, s pohybem klientů
  - Malé hodnoty – minuty až hodiny

DHCP options

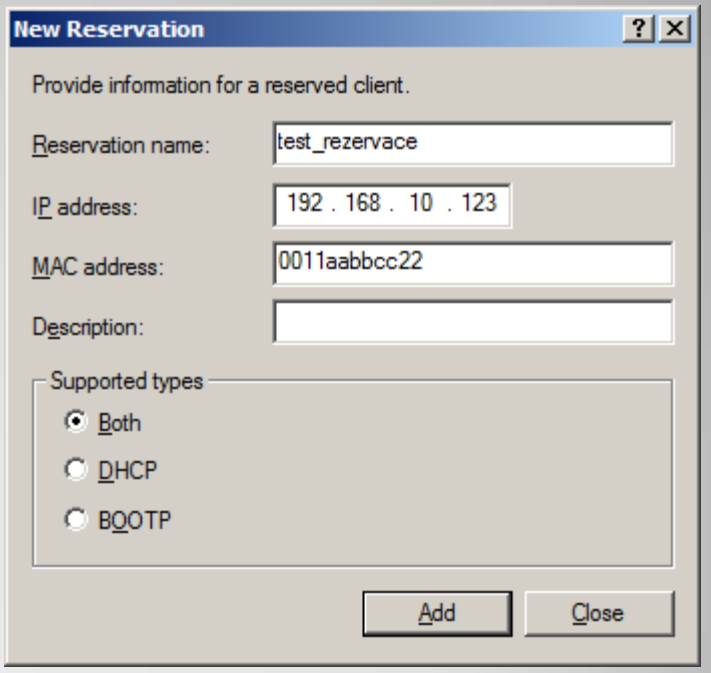
- Jedná se o další parametry pro klienty
- Až několik desítek nastavení
- Nejčastěji:
  - Router (výchozí brána) … 003
  - DNS server … 006
  - Název domény (DNS suffix) … 015

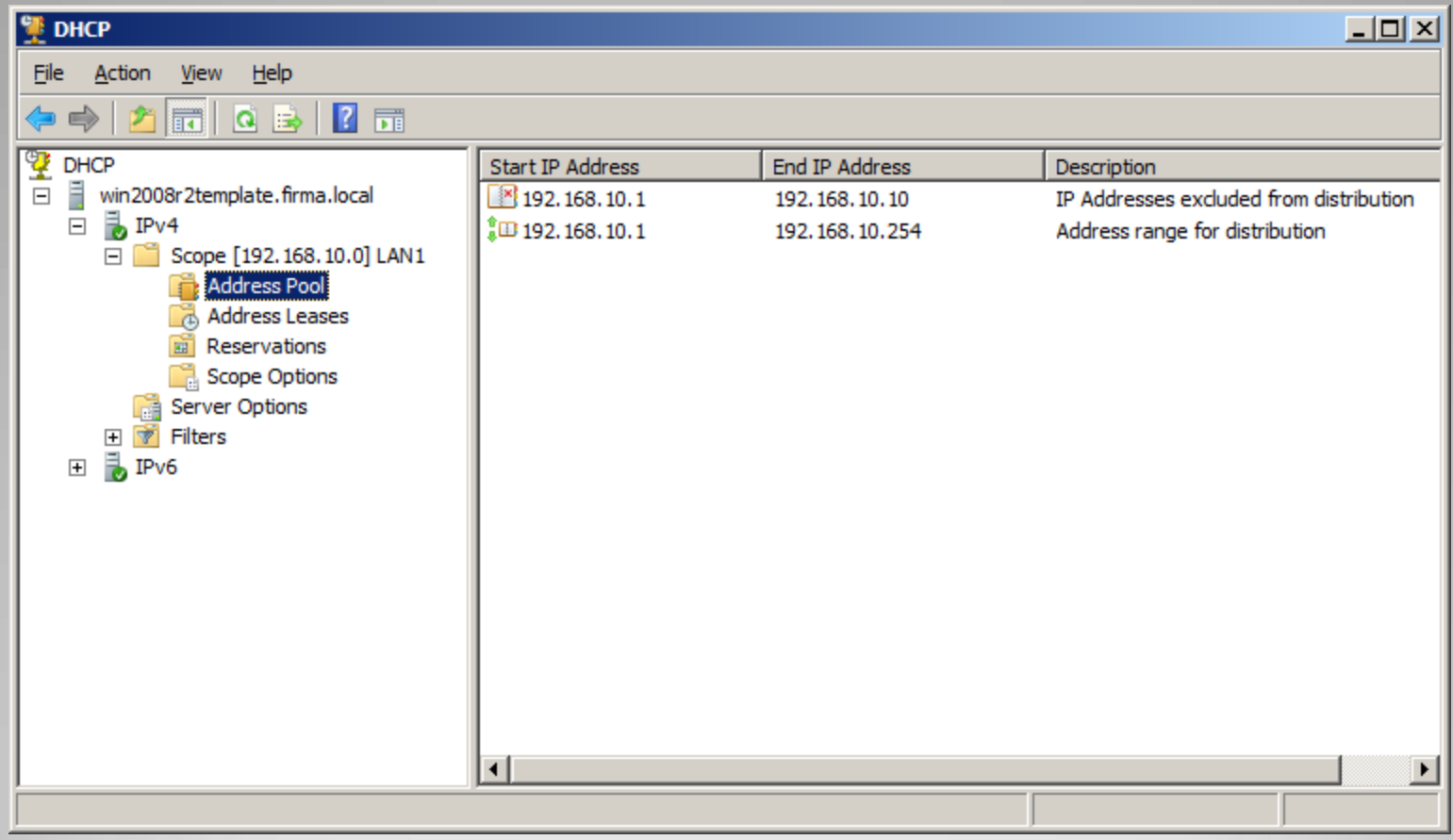
DHCP options

- Nastavení na úrovni serveru
  - Ovlivní všechny scope
  - Nastavení pro všechny subnety
- Nastavení na úrovni scope
  - Pouze pro konkrétní subnet
  - Má prioritu
- Nastavení na úrovni rezervace
  - Málo využívané
  - Ovlivní pouze jednoho klienta

DHCP rezervace

- Pevná IP adresa pro vybraného klienta
- Přiděluje se na základě MAC adresy
- Pouze v rámci subnetu




DHCP
File
Action
View
Help
DHCP
win2008r2template.firma.local
IPv4
Scope [192.168.10.0] LAN1
Address Pool
Address Leases
Reservations
Scope Options
Server Options
Filters
IPv6
Start IP Address
End IP Address
Description
192.168.10.1
192.168.10.10
IP Addresses excluded from distribution
192.168.10.1
192.168.10.254
Address range for distribution

DHCP

DHCP

- Pro zajištění vysoké dostupnosti DHCP
- Alespoň dva DHCP servery
- Scope rozděleny
  - Win2008 R2 nabízí funkci „split scope“
- Běžně DHCP server obsluhuje několik subnetů
- Relay agent předává DHCP pakety

DHCP klient

- MS DHCP klient – broadcast komunikace

- Užitečné příkazy:
- IPCONFIG /RELEASE
  - Uvolní DHCP konfiguraci z klienta
- IPCONFIG /RENEW
  - Opětovně zažádá o DHCP konfiguraci