Serverové systémy Microsoft Windows

IW2/XMW2 2010/2011

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 16.2.2011

Systém DNS

Systém DNS (Domain Name System)

- Zajišťuje překlad doménových jmen na IP adresy a opačně (IP adres na doménová jména)
- Zjednodušuje identifikaci počítačů
  - Použití textových názvů namísto číselných IP adres
- Umožňuje transparentní změny IP adres
  - Doménová jména se nemění, pouze jejich překlad
- Lze výhodně použít pro
  - Vyvažování výkonu (*load balancing*)
  - Rozlišování služeb (známé prefixy služeb, např. ***www***)

Architektura DNS

- Decentralizovaný klient-server systém
  - DNS záznamy jsou rozprostřeny po více serverech
  - Komunikace pomocí protokolu UDP (port 53)
- Hierarchický systém
  - Doménová jména tvoří stromový prostor jmen

Hierarchie DNS

- Prostor doménových jmen tvoří obecný strom
  - Kořenovým uzlem stromu (*the root*) je prázdný uzel
  - Nekořenové uzly stromu označují názvy domén nebo počítačů (*hostname*)
  - Strom může mít maximálně 127 úrovní (hloubku)
- Názvy uzlů stromu
  - Mohou obsahovat maximálně 63 znaků
  - Nesmí obsahovat tečky
  - Se mohou opakovat (v jiných úrovních nebo větvích)

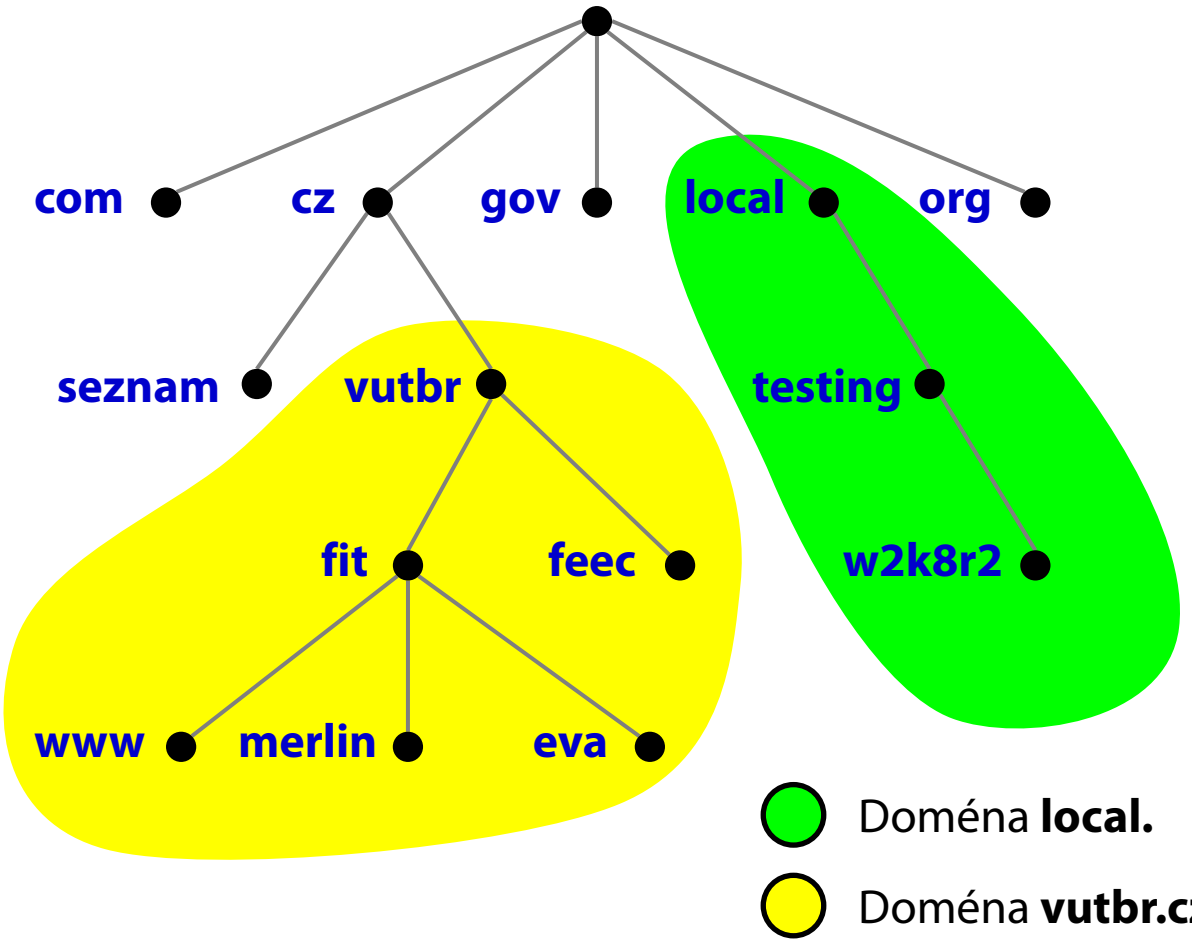
Doménová jména (Domain Names)

- Textové řetězce identifikující počítače v síti
  - Mohou obsahovat maximálně 255 znaků
  - Rozděleny do částí oddělených tečkou
- Plně kvalifikovaná doménová jména (FQDN, *Fully Qualified Domain Names*)
  - Sekvence uzlů z listového uzlu do kořenového uzlu
- Částečně kvalifikovaná doménová jména (PQDN, *Partially Qualified Domain Names*)
  - Sekvence uzlů z listového uzlu do konkrétní domény

Domény

- Podstromy stromu doménových jmen
- Dělí prostor doménových jmen na menší celky
  - Zjednodušení administrace
- Názvy domén
  - Sekvence uzlů z nelistového uzlu do kořenového uzlu
  - Nemohou být částečně kvalifikované
- Subdomény
  - Domény, jenž jsou součástí větší (rozsáhlejší) domény
  - Podstromy domén

Příklad prostoru doménových jmen



Příklady FQDN jmen
www.fit.vutbr.cz.
eva.fit.vutbr.cz.
w2k8r2.testing.local.

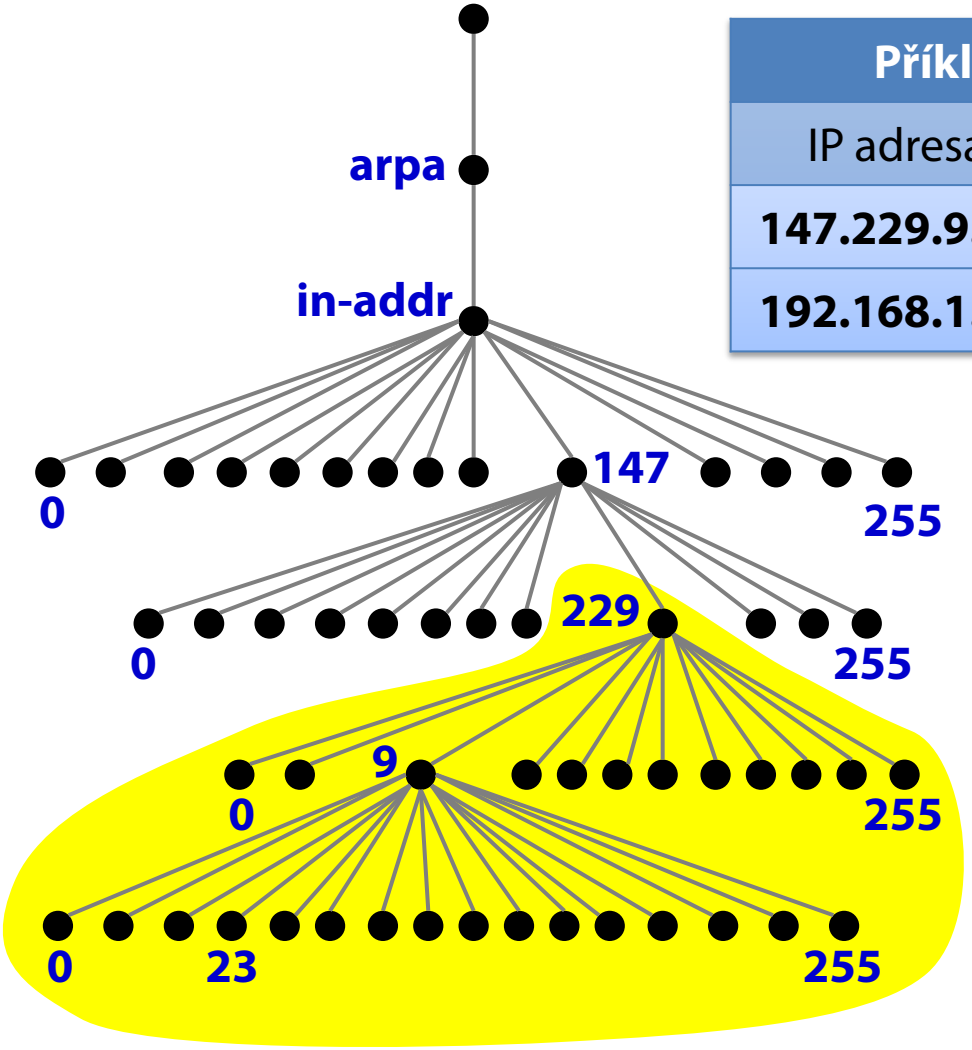
Příklady PQDN jmen (doména vutbr.cz.)
eva.fit
www.fit

Příklady subdomén (doména vutbr.cz.)
fit.vutbr.cz.
feec.vutbr.cz.

Reverzní mapování

- Překlad IP adres zpět na doménová jména
- Využívá se pro ověření validity překladu
- IP adresy uloženy ve formě PQDN v doménách
  - **in-addr.arpa.** pro IPv4 adresy
  - **ip6.arpa.** pro IPv6 adresy
- Převod IP adres na PQDN probíhá v obráceném pořadí (od nejvyššího bitu IP adresy) po
  - **8 bitech** pro IPv4 adresy
  - **4 bitech** pro IPv6 adresy

Příklad reverzního mapování pro IPv4



Příklady FQDN jmen pro IPv4 adresy	
IP adresa	FQDN jméno
147.229.9.23	**23.9.229.147.in-addr.arpa.**
192.168.1.10	**10.1.168.192.in-addr.arpa.**

Doména **229.147.in-addr.arpa.**

DNS odpovědi

- Rozdělení z hlediska aktuálností informací
  - Autoritativní odpověď
    - Obsahuje vždy aktuální informace
  - Neautoritativní odpověď
    - Může obsahovat již neplatné informace
- Rozdělení z hlediska typu informací
  - Pozitivní odpověď
    - Obsahuje záznam(y) pro dotazované doménové jméno
  - Negativní odpověď
    - Dotazované doménové jméno neexistuje / je jiného typu

DNS zóny

- Rozdělení podle směru překladu
  - Dopředná (*Forward lookup*) zóna
    - Překlad doménových jmen na IP adresy
  - Zpětná (*Reverse lookup*) zóna
    - Překlad IP adres na doménová jména
- Rozdělení podle obsahu
  - Primární zóna (standardní nebo integrovaná v AD)
  - Sekundární zóna
  - Stub zóna

Primární zóna

- Obsahuje veškeré záznamy pro danou doménu
- Umožňuje přímou modifikaci DNS záznamů
- Je vždy autoritativní
- Standardní primární zóna
  - Ukládá DNS záznamy v textové podobě v zónových souborech **<*systém*>\System32\dns\<*doména*>.dns**
- Primární zóna integrovaná v Active Directory
  - Ukládá DNS záznamy jako objekty do databáze Active Directory do kontejneru **dnsZone**

Sekundární a stub zóna

- Sekundární zóna
  - Obsahuje veškeré záznamy pro danou doménu
  - DNS záznamy jsou určeny pouze pro čtení
  - Modifikace DNS záznamů pouze pomocí přenosu zón
  - Je vždy autoritativní
- Stub zóna
  - Obsahuje jen informace pro lokalizaci autoritativních DNS serverů (**SOA** a **NS** + **A** nebo **AAAA** záznamy)
  - Není autoritativní

DNS servery

- Primární DNS server
  - Obsahuje primární zónu
  - Vždy autoritativní
- Sekundární DNS server
  - Obsahuje sekundární zónu
  - Vždy autoritativní
- Záložní (*Caching-Only*) DNS server
  - Obsahuje stub zónu
  - Není autoritativní

Záložní (Caching-Only) DNS server

- Kešuje informace o překladu doménových jmen na IP adresy (a naopak) ve vyrovnávací paměti
  - Pokud lze požadavek na překlad vyřídit pomocí údajů ve vyrovnávací paměti, vytvoří odpověď
  - Jinak zašle požadavek na překlad jinému DNS serveru a odpověď uloží do vyrovnávací paměti
- Vhodný pro urychlení překladu mezi místy, které mají špatnou konektivitu

DNS záznamy (DNS records)

- A (Address)
- AAAA (IPv6 Address)
- CNAME (Canonical Name)
- MX (Mail Exchange)
- NS (Name Server)
- PTR (Pointer)
- SOA (Start of Authority)
- …

A a AAAA záznamy

- A (Address) záznam
  - Mapuje doménové jméno na IPv4 adresu
  - Formát

<doménové jméno>* IN A *<IPv4 adresa>

- AAAA (IPv6 Address) záznam
  - Mapuje doménové jméno na IPv6 adresu
  - Formát

<doménové jméno>* IN AAAA *<IPv6 adresa>

CNAME a MX záznamy

- CNAME (Canonical Name)
  - Mapuje doménové jméno na jiné doménové jméno
  - Formát

<zdojové domémové jméno>* IN CNAME *<cílové domémové jméno>

- MX (Mail Exchange)
  - Mapuje název domény na doménové jméno serveru pro příjem elektronické pošty
  - Formát

<doména>* IN MX *<priorita>* *<domémové jméno>

NS a PTR záznamy

- NS (Name Server)
  - Mapuje název domény na doménové jméno serveru DNS, jenž je autoritativní pro tuto doménu
  - Formát

<doména>* IN NS *<domémové jméno>

- PTR (Pointer)
  - Mapuje IP adresu na doménové jméno
  - Formát

<in-addr.arpa/ip6.arpa domémové jméno>* IN PTR *<domémové jméno>

SOA záznam

- Mapuje název domény na základní informace o této doméně
- Formát

<doména> **IN SOA** ***<primární DNS server>*** ***<email>*** **(**	
<serial>	Sériové číslo zóny, inkrementace při každé změně obsahu zóny
<refresh>	Interval dotazování sekundárního serveru na změny zóny
<retry>	Doba opětovného dotazování na změny zóny po nezdaru
<expire>	Doba platnosti záznamů sekundárního serveru
<ttl>**)**	Doba platnosti jednotlivých záznamů ve vyrovnávací paměti

Přenos zón (Zone Transfer)

- Synchronizace obsahu zóny mezi dvěma servery DNS, primárním (*master*) a sekundárním (*slave*)
- Aktualizace jednoho originálu (*single-master*)
  - Vyžaduje přítomnost jediné primární zóny
- Využívá protokol TCP (port 53)
- Dva způsoby přenosu zón
  - Úplný přenos zóny (AXFR)
  - Inkrementální přenos zóny (IXFR)

Zjišťování změn

- Pomocí dotazování (*pull* metoda)
  - Slave server se v pravidelných intervalech dotazuje master serveru na jeho záznam SOA
  - Slave server porovná sériové čísla v obou záznamech SOA (svém a od master serveru)
  - Pokud je sériové číslo v záznamu SOA master serveru vyšší než u slave serveru, provede se přenos zón
- Pomocí oznámení (*push* metoda)
  - Master server při změně zašle všem slave serverům oznámení a ty provedou přenos zón push metodou

Metody přenosu zón

- Úplný přenos zón (AXFR)
  - Přenáší se všechny DNS záznamy
  - Provádí se nejčastěji po vytvoření sekundárního DNS serveru
- Inkrementální přenos zón (IXFR)
  - Přenáší se pouze ty DNS záznamy, jenž byly změněny od posledního přenosu zón
  - Výchozí způsob přenosu zón

Integrace DNS a Active Directory

- Využití replikace Active Directory pro přenos zón
  - Podpora existence více primárních zón (aktualizace více originálů, *multi-master*)
  - Možnost replikace pouze na určité DNS servery
  - Podpora komprese přenášených dat
- Vyšší bezpečnost DNS záznamů
  - Omezování přístupu k záznamům zóny pomocí ACL (*Access Control List*) seznamů
- Umožňuje zabezpečenou dynamickou aktualizaci DNS záznamů (*secure dynamic updates*)

Dynamické aktualizace DNS záznamů

- Automatická registrace klienta u DNS serveru
  - Vložení A resp. AAAA, případně PTR záznamů
  - Může provést i DHCP server namísto klienta
  - V Active Directory lze požadovat autentizaci klienta
- Lze provádět pouze u primárního DNS serveru
  - Sekundární DNS server místo registrace vrací adresu primárního DNS serveru, jenž může registraci provést
- Manuální registrace klienta
  - **ipconfig /registerdns**

Překlad jmen (name resolution)

- Překlad hostitelských jmen (*hostnames*) počítačů na odpovídající IP adresy a naopak
- Zajišťuje služba Klient DNS
- Tři základní technologie pro překlad jmen
  - Systém DNS
  - LLMNR
  - Systém NetBIOS a služba WINS

Postup překladu hostitelského jména

1) Ověření lokálního hostitelského jména
2) Prohledání vyrovnávací paměti klienta DNS
3) Dotazování pomocí systému DNS
4) Prohledání vyrovnávací paměti LLMNR
5) Dotazování pomocí LLMNR
6) Prohledání vyrovnávací paměti NetBIOS
7) Dotazování pomocí systému WINS
8) Dotazování pomocí NetBIOS
9) Prohledání souboru **lmhosts**

Překlad jmen pomocí systému DNS

- Podpora negativního kešování (*negative caching*)
  - Zaznamenávání informací o neúspěšných překladech
- Podpora statického mapování jmen
  - Soubor ***<systém>*\System32\drivers\etc\hosts**
- Zaslání dotazu DNS serveru
  - **nslookup *<doménové-jméno>***
- Vytváření doménových jmen
  - Každý počítač může mít přiřazen seznam domén
  - Připojování názvů domén k hostitelskému jménu

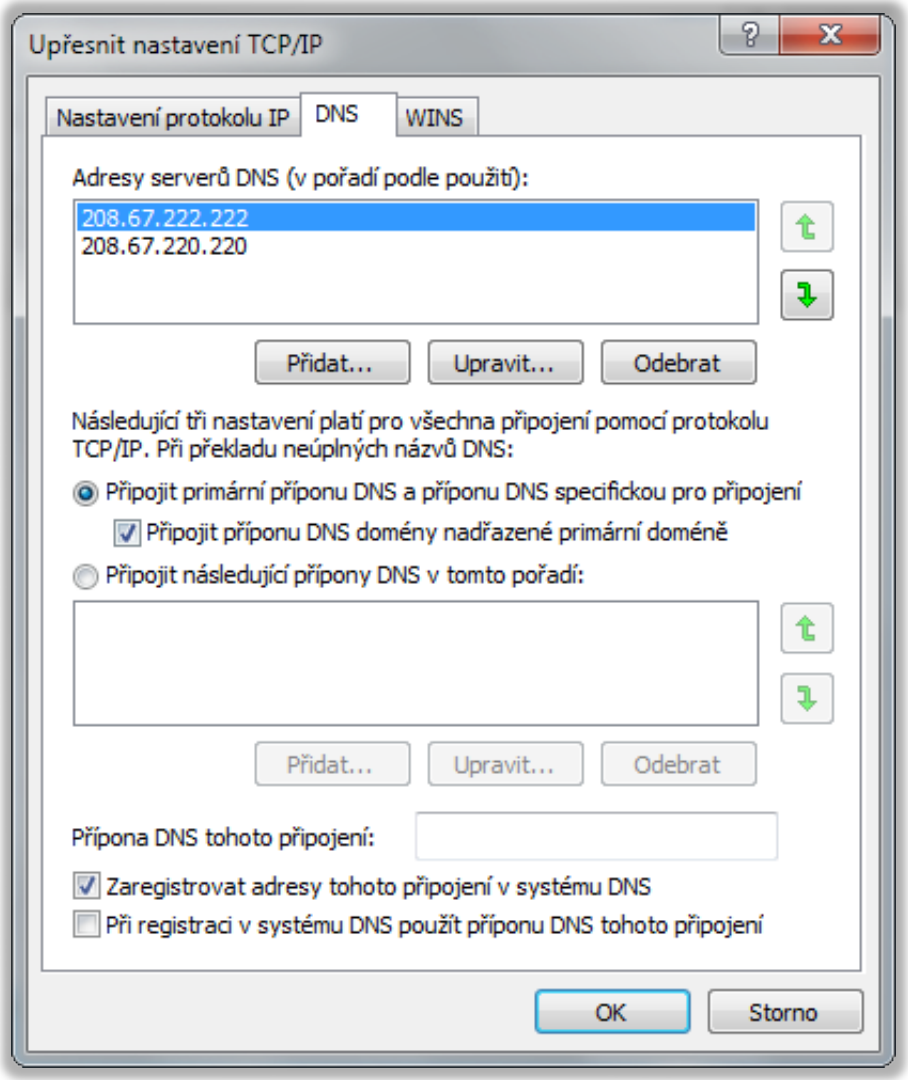
Překlad pomocí LLMNR

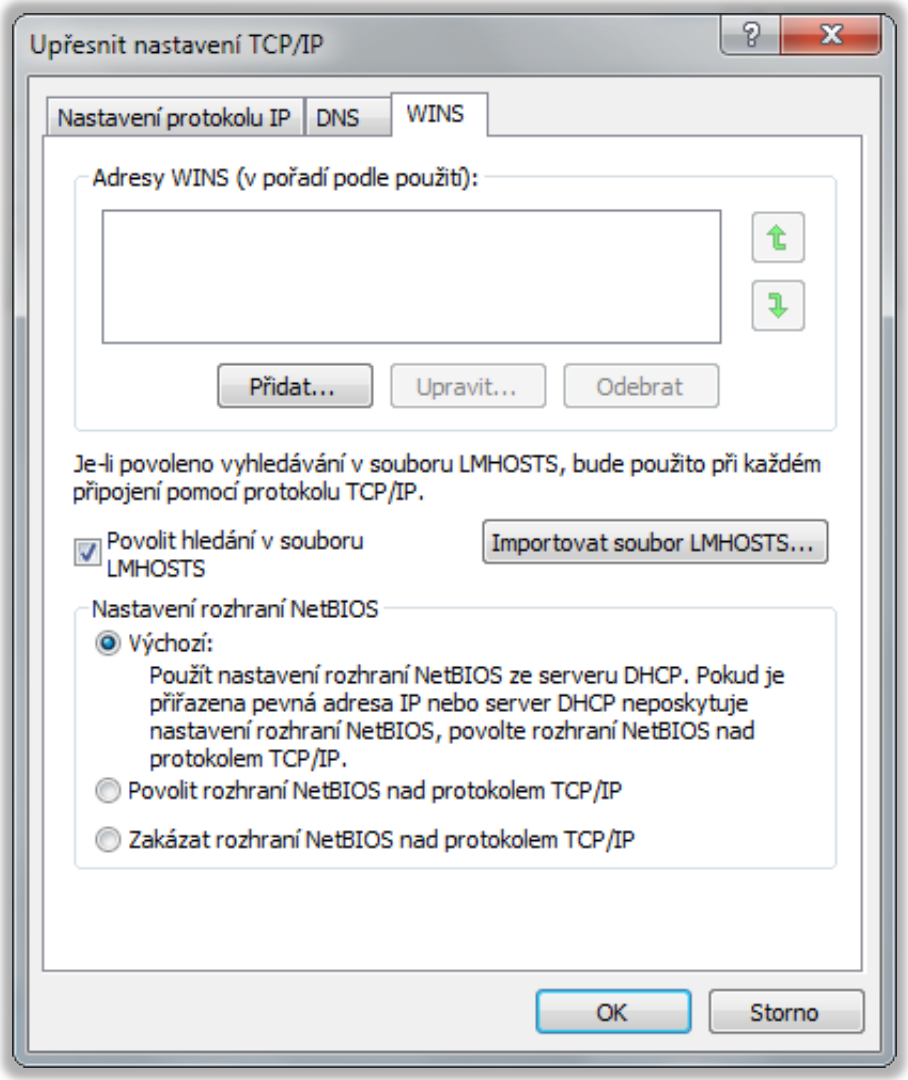
- LLMNR (*Link Local Multicast Name Resolution*)
  - Překlad s využitím (linkových) skupinových IP adres
- Využívá službu zjišťování sítě (*Network Discovery*)
- Princip překladu
  - Počítač (Klient DNS) zašle všem počítačům požadavek na překlad hostitelského jména
  - Počítač mající hledané hostitelské jméno odpoví svou IP adresou (IP adresou rozhraní na dané lince)

Překlad pomocí NetBIOS a WINS

- NetBIOS (NetBIOS nad protokolem TCP/IP)
  - Překlad s využitím plochého (*flat*) jmenného systému
  - NetBIOS jména mohou mít maximálně 15 znaků
- Požadavky pro překlad
  - Musí být povolen NetBIOS nad protokolem TCP/IP
  - Překládaný název nesmí být delší než 15 znaků
  - Překládaný název nesmí být doménové jméno
- WINS (*Windows Internet Naming Service*)
  - Mapuje NetBIOS jména na odpovídající IPv4 adresy

Nastavení DNS, NetBIOS a WINS





Vyrovnávací paměti DNS a NetBIOS

- Zobrazení obsahu vyrovnávací paměti DNS
  - **ipconfig /displaydns**
- Vymazání obsahu vyrovnávací paměti DNS
  - **ipconfig /flushdns**
- Zobrazení obsahu vyrovnávací paměti NetBIOS
  - **nbtstat -c**
- Vymazání obsahu vyrovnávací paměti NetBIOS
  - **nbtstat -R**

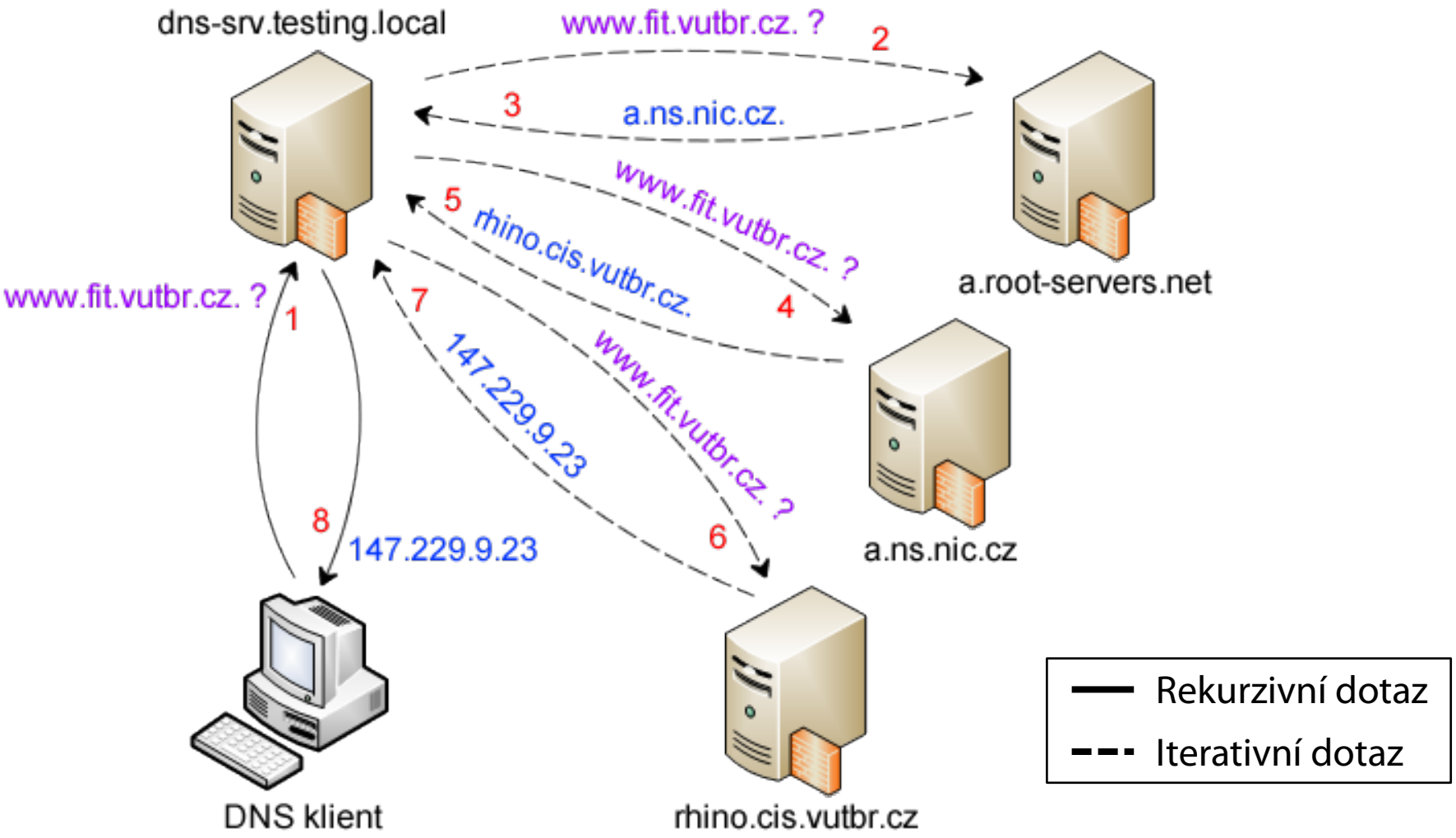
Zóna globálních jmen

- Zóna s názvem **GlobalNames**
  - Musí být integrovaná v Active Directory
- Může obsahovat pouze CNAME záznamy
  - Nesmí mít povoleny dynamické aktualizace záznamů
- Částečně nahrazuje WINS servery
  - Názvy mohou být maximálně 15 znaků dlouhé
- Replikace probíhá na úrovni celého lesa (*forest*)
  - Musí být povolena na každém řadiči domény

DNS dotazy

- Každý dotaz obsahuje
  - Plně kvalifikované doménové jméno (FQDN)
  - Typ dotazu (např. požadovaný typ záznamu)
  - Třídu doménového jména (prakticky vždy internet)
- Rekurzivní dotaz
  - Pokud DNS server nezná odpověď, vrátí chybu
- Iterativní dotaz
  - Pokud DNS server nezná odpověď, vrátí adresy DNS serverů, jenž by ji mohly znát

Ilustrace dotazování pomocí DNS



DNS forwarding

- Přeposílání DNS dotazů nezodpovězených daným DNS serverem na jiné DNS servery
  - Ve výchozím nastavení na kořenové DNS servery
- Podmíněné přeposílání (*conditional forwarding*)
  - Přeposílání dotazů pouze pro specifickou doménu
  - Urychluje překlad a snižuje zátěž DNS serveru
- Vytvoření podmíněného přeposílání (*forwarder*)
  - Příkazem **dnscmd <*dns-server*> /zoneadd <*doména*> /forwarder <*ip*>** nebo přes DNS konzoli

Vyvažování výkonu (load balancing)

- Navrácení různých IP adres pro stejné doménové jméno (rozložení komunikace mezí více počítačů)
- Realizováno pomocí sady A resp. AAAA záznamů
  - Každý záznam překládá doménové jméno na jinou IP adresu, při každém dotazu vybrán jiný záznam
  - Výběr záznamů probíhá cyklicky (tzv. *round robin*)
- Nebere v úvahu
  - Vytížení jednotlivých serverů
  - Kontinuitu služeb

Protokol DHCP

Protokol DHCP

- DHCP (*Dynamic Host Configuration Protocol*)
- Protokol pro automatickou konfiguraci síťových rozhraní (a počítačů)
  - Přidělování IP adres a masek resp. prefixů podsítě
- Využívá všesměrové vysílání a protokol UDP
  - Port 67 pro komunikaci s DHCP servery
  - Port 68 pro komunikaci s DHCP klienty

DHCP server

- Přiřazuje IP adresy z určitého rozsahu (*scope*)
  - Musí mít IP adresu z poskytovaného rozsahu IP adres
- Spravuje rezervace
  - Přiřazování IP adres na základě MAC adres rozhraní
- Umožňuje navíc nastavit např.
  - Výchozí bránu (003 Router)
  - DNS servery (006 DNS servers)
  - Název domény (015 Domain name)
  - WINS servery (044 WINS/NBNS servers)

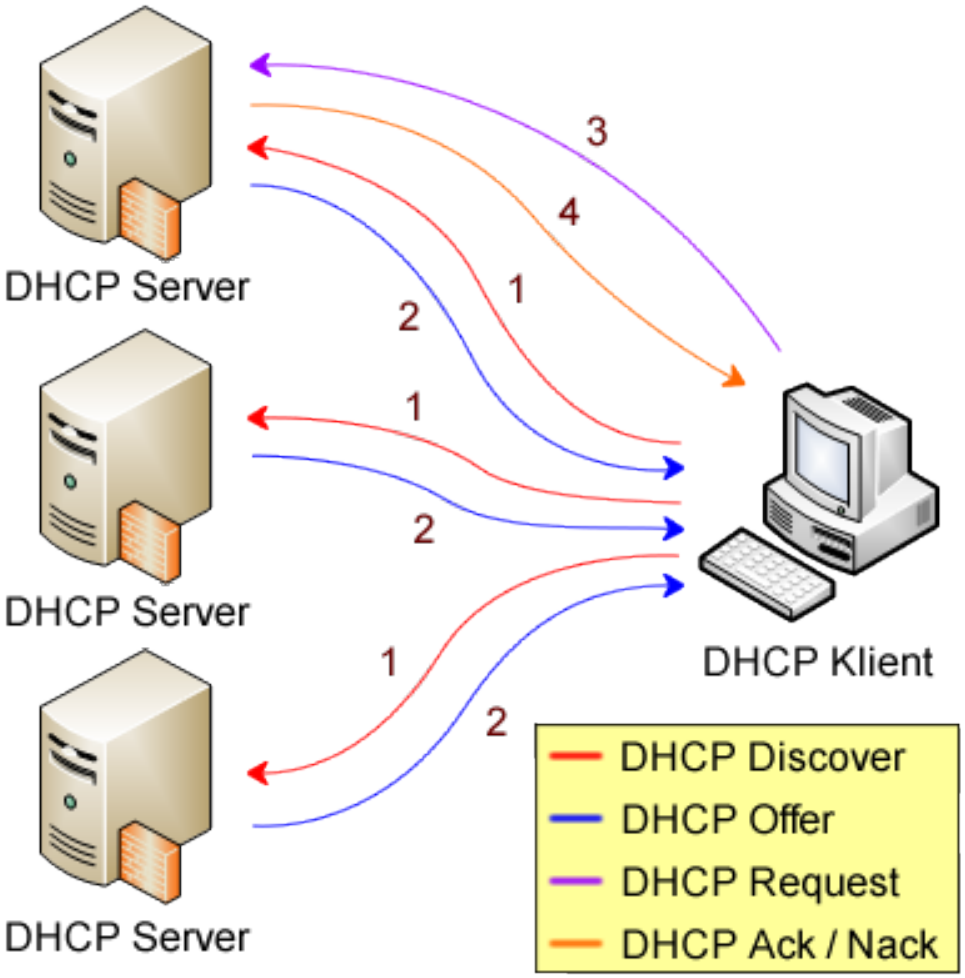
DHCP server v doméně

- Nutnost autorizace serveru v Active Directory
  - Vyžaduje oprávnění uživatelů ze skupiny Enterprise Admins (nejvyšší správci Active Directory)
  - Neautorizované servery nesmí přidělovat IP adresy
  - Ochrana proti tzv. Rogue DHCP serverům
- Autorizace DHCP serveru
  - Přes DHCP konzoli
  - Příkazem **netsh dhcp server <*název/ip*> initiate auth**

DHCP nastavení (DHCP options)

- Specifikace na úrovni
  - Celého DHCP serveru
  - Konkrétního rozsahu (*scope*)
  - Jednotlivých rezervací
- Možnost filtrování na základě
  - Třídy definované výrobcem (*vendor-defined class*)
    - Určuje DHCP klient (060 Vendor Class ID)
  - Třídy definované uživatelem (*user-defined class*)
    - Nastavení pomocí **ipconfig /setclassid *<rozhraní>* *<název>***

Ilustrace přidělování IP adres



Přidělení nové IP adresy	
1	DHCP Discover
2	DHCP Offer
3	DHCP Request
4	DHCP Ack / Nack

Prodloužení výpůjčky	
1	DHCP Request
2	DHCP Ack / Nack

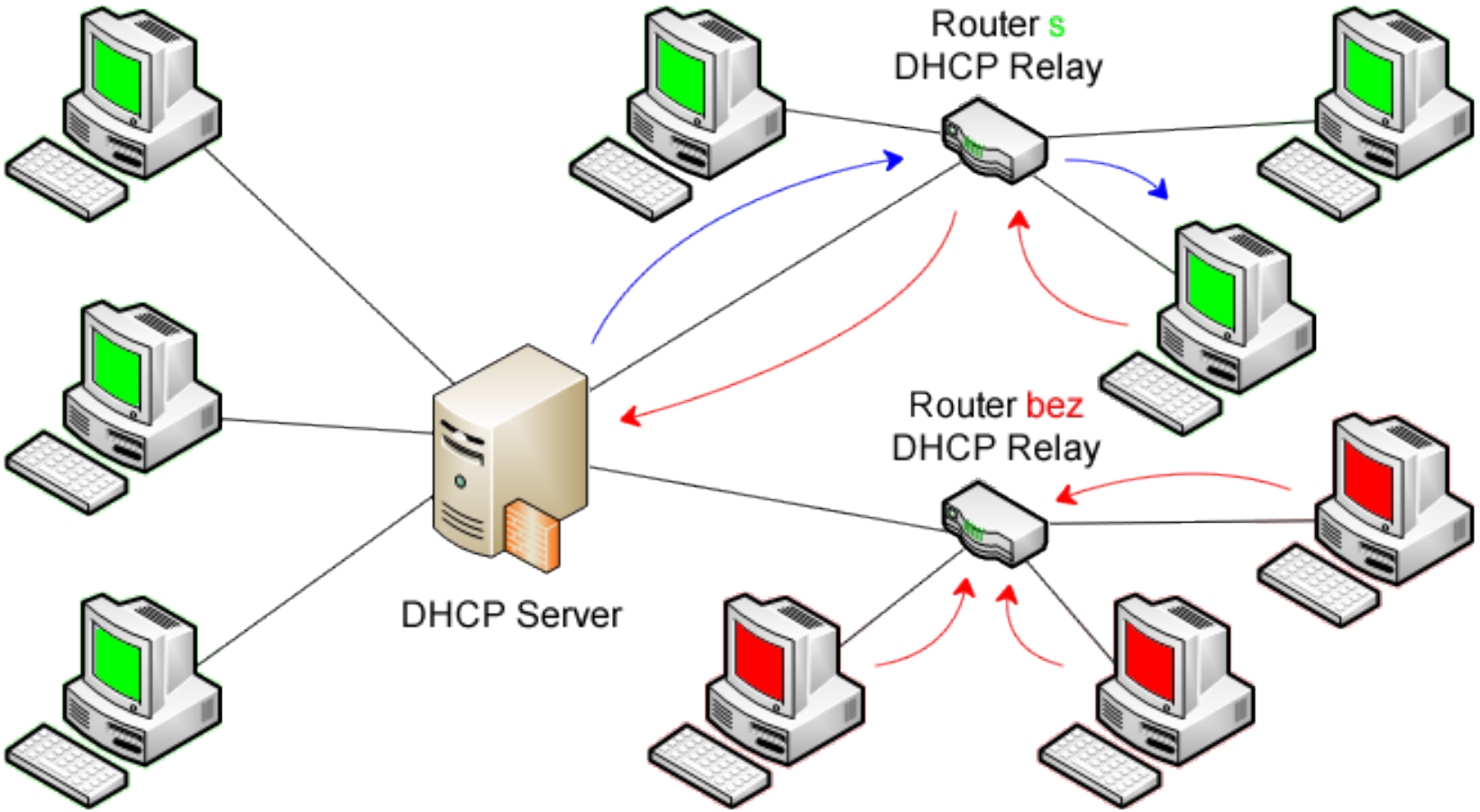
Postup přidělování IP adres

1) DHCP klient zašle všesměrovou zprávu **DHCP Discover** všem DHCP serverům na síti DHCP klienta
2) Každý DHCP server odpoví všesměrovou zprávou **DHCP Offer** obsahující jim nabízenou IP adresu
3) DHCP klient z přijatých nabídek vybere jednu a potvrdí svůj zájem o její zapůjčení všesměrovou zprávou **DHCP Request**
4) DHCP server zapůjčení nabídnuté IP adresy buď stvrdí zprávou **DHCP Ack** nebo odmítne zprávou **DHCP Nack**

Prodlužování výpůjčky (*lease renewal*)

- IP adresy jsou zapůjčeny jen na určitou dobu, tzv. dobu výpůjčky (*lease time*)
  - Nutno pravidelně tuto dobu prodlužovat opětovným zasíláním zpráv **DHCP Request**
- Prodloužení doby výpůjčky probíhá
  - Po uplynutí 50% doby výpůjčky u DHCP serveru, jenž zapůjčil danou IP adresu (používá *unicast*)
  - Po uplynutí 87,5% doby výpůjčky u jakéhokoliv DHCP serveru (používá *broadcast*)

DHCP relay

- Umožňuje DHCP klientům komunikovat s DHCP servery umístěnými na jiné síti
- Směruje DHCP zprávy z jedné sítě do jiné
  - Na síti s DHCP klienty se chová jako DHCP server
  - Na síti s DHCP serverem přeposílá požadavky tomuto serveru a přijímá odpovědi
- Pro komunikaci s DHCP servery používá *unicast*
  - IP adresa DHCP relay uložena zvlášť v poli **GIADDR**

Ilustrace DHCP relay