# 11. DHCP a DNS

## Teoretická část

**Vysvětlete a popište protokoly DHCP a DNS. Vysvětlete přidělování IP adres (statické, dynamické, dynamické rezervované), včetně DHCP server a klient.** **Vysvětlete strukturu překladu DNS (host/domain name na IP adresu).** **Vysvětlete hierarchický systém doménových jmen.**

## Praktická část

1. **V úloze SVR2008A předveďte a popište nastavení DNS serveru. (Na serveru)**
2. **V úloze SVR2008A předveďte a popište nastavení DHCP serveru včetně DHCP scopes. (Na serveru)**
3. **V Excel dokumentu předveďte tvorbu IP pool vč. DNS záznamu. (V excelu: IP a k tomu jméno)**

## Doplňující otázky

1. **Vyjmenujte a popište typy záznamů na DNS serveru.**
2. **Specifikujte typy zón na DNS serveru.**
3. **Na host PC předveďte nastavení DHCP klienta. (Na kartě)**

<http://digilib.k.utb.cz/bitstream/handle/10563/16471/habrman_2011_bp.pdf?sequence=1> (Nastavení DNS a DHCP na serveru)

# DHCP

DHCP(Dynamic Host Configuration Protocol) protokol umožňuje prostřednictvím DHCP serveru nastavovat stanicím v počítačové síti sadu parametrů nutných pro komunikaci pomocí IP protokolu (tj. využívat rodinu protokolů TCP/IP). Umožňuje předávat i doplňující a uživatelsky definované parametry. Významným způsobem tak zjednodušuje a centralizuje správu počítačové sítě (například při přidávání nových stanic, hromadné změně parametrů nebo pro skrytí technických detailů před uživateli). DHCP servery mohou být sdruženy do skupin, aby bylo přidělování adres odolné vůči výpadkům. Pokud klient některým parametrům nerozumí, ignoruje je.

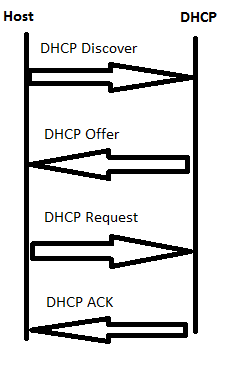
Typicky se pomocí DHCP nastavují tyto parametry:

* IP adresa
* maska sítě
* implicitní brána (anglicky default gateway)
* DNS server (seznam jedné nebo více IP adres DNS serverů)
* a další údaje

# Zpětná kompatibilita - BOOTP

Protokol DHCP nebyl se svým předchůdcem BOOTP zpětně kompatibilní, což je pro internetové protokoly a vydávání RFC velmi nezvyklé. Protokol DHCP přinesl pouze možnost „pronájmu IP adresy“. Vzhledem k modularitě BOOTP protokolu ale bylo možné tuto vlastnost implementovat i do tohoto předchůdce. Zpětně nekompatibilní protokol prosadila firma Microsoft, která pro systémy Windows 95 a novější implementovala jako standardní součást pouze podporu protokolu DHCP. Pro správce tak bylo tehdy nutné společně s novou verzí stolního systému Windows nakoupit a provozovat též serverovou edici Windows NT, protože podpora DHCP byla do stávajících BOOTP serverů (typicky provozovaných na unixových systémech) implementována až se zpožděním.

# Princip činnosti

Klienti žádají server o IP adresu, ten u každého klienta eviduje půjčenou IP adresu a čas, do kdy ji klient smí používat (doba zapůjčení, anglicky lease time). Poté co vyprší, smí server adresu přidělovat jiným klientům. Klient komunikuje na UDP portu 68, server naslouchá na UDP portu 67.

1. Po připojení do sítě klient vyšle broadcastem **DHCP DISCOVER** paket.
2. Na ten odpoví DHCP server paketem **DHCP OFFER** s nabídkou IP adresy.
3. Klient si z (teoreticky několika) nabídek vybere jednu IP adresu a o tu požádá paketem **DHCP REQUEST**.
4. Server mu ji vzápětí potvrdí odpovědí **DHCP ACK**. Jakmile klient obdrží DHCP ACK, může už IP adresu a zbylá nastavení používat.
5. Klient musí před uplynutím doby zapůjčení z DHCP ACK obnovit svou IP adresu.
6. Pokud lhůta uplyne, aniž by dostal nové potvrzení, klient musí IP adresu přestat používat.

# Možnosti přidělení IP adresy

IP adresa může být stanici přidělena několika způsoby:

* Ruční nastavení - V tomto případě správce sítě nevyužívá DHCP serveru a konfiguraci jednotlivých stanic zapisuje jednotlivě přímo do konfigurace jednotlivých stanic.
* Statická alokace - DHCP server obsahuje seznam MAC adres a k nim příslušným IP adres. Pokud je žádající stanice v seznamu, dostane vždy přidělenu stejnou pevně definovanou IP adresu.
* Dynamická alokace - Správce sítě na DHCP serveru vymezí rozsah adres, které budou přidělovány stanicím, které nejsou registrovány. Časové omezení pronájmu IP adresy dovoluje DHCP serveru již nepoužívané adresy přidělovat jiným stanicím. Registrace dříve pronajatých IP adres umožňuje DHCP serveru při příštím pronájmu přidělit stejnou IP adresu. V IPv6 sítích je automatickému nastavení stanice věnována vyšší pozornost, aby byla konfigurace počítačové sítě ještě jednodušší.

# DNS

**DNS (systém doménových jmen)** je jednou z technologií, které se ve světě počítačových sítí vyskytují a vyvíjí téměř 30 let. Za tuto dobu si nabyla neotřesitelnou pozici jak při překládání doménových jmen na adresy IP, tak v procesu opačném. Přesný počet serverů, které jsou do DNS infrastruktury na internetu zapojené, je, podobně jako exaktní počty DNS dotazů a odpovědí které tyto servery denně obsluhují, prakticky nemožné zjistit. Několik takových serverů totiž ve své síti má nejen každý poskytovatel internetové konektivity a doménových služeb, ale i mnohé společnosti a i některé domácnosti.

**DNS (Domain Name System) je hierarchický systém**[**doménových jmen**](https://cs.wikipedia.org/wiki/Dom%C3%A9nov%C3%A9_jm%C3%A9no), který je **realizován servery DNS** a **protokolem stejného jména**, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou **vzájemné převody doménových jmen a**[**IP adres**](https://cs.wikipedia.org/wiki/IP_adresa) [uzlů sítě](https://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%BD_uzel). Později ale přibral další funkce (např. pro elektronickou poštu či IP telefonii) a slouží dnes de fakto jako **distribuovaná databáze síťových informací**.

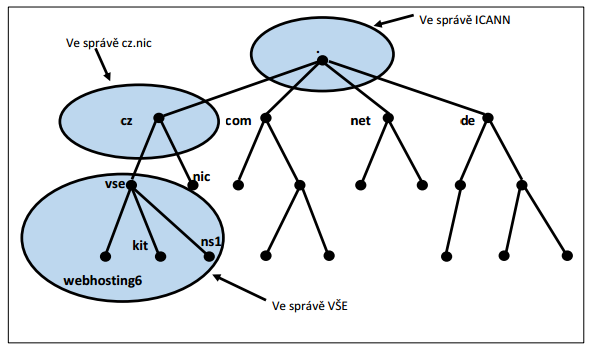
Protokol používá **porty**[**TCP**](https://cs.wikipedia.org/wiki/Transmission_Control_Protocol)**/53 i**[**UDP**](https://cs.wikipedia.org/wiki/User_Datagram_Protocol)**/53**, je definován v [RFC1035](http://www.faqs.org/rfcs/rfc1035.html). Servery DNS jsou organizovány hierarchicky, stejně jako jsou hierarchicky tvořeny [názvy domén](https://cs.wikipedia.org/wiki/Internetov%C3%A1_dom%C3%A9na). Jména domén umožňují lepší orientaci lidem, **adresy pro stroje jsou však vyjádřeny pomocí adres 32bitových (**[**IPv4**](https://cs.wikipedia.org/wiki/TCP/IP#IPv4)**) A záznam nebo 128bitových** ([IPv6](https://cs.wikipedia.org/wiki/TCP/IP#IPv6)) - AAAA záznam. Systém DNS umožňuje efektivně udržovat decentralizované databáze doménových jmen a jejich překlad na IP adresy. Stejně tak zajišťuje zpětný překlad IP adresy na doménové jméno - PTR záznam.

# Historie DNS

Protože je používání názvů pro člověka daleko příjemnější než používání číselných adres, vznikla už v dobách [ARPANETu](https://cs.wikipedia.org/wiki/ARPANET) potřeba takový převod realizovat. Původně byl na všechny počítače distribuován jediný soubor (v Unixu /etc/**hosts**). Tato koncepce přestala velmi rychle vyhovovat potřebám a především nárokům na rychlou aktualizaci. Přesto se tento soubor dodnes používá, v závislosti na konfiguraci systému je možné jej použít buď prioritně před dotazem na DNS nebo v případě, že DNS neodpovídá. Je možné jej také použít k uložení vlastních přezdívek pro často navštěvované servery, případně také pro blokování reklam a podobně.

# Hierarchický systém doménových jmen

DNS v internetu jako celek je možné označit za decentralizovanou databázi. Decentralizovaná je proto, že nikdo, tedy žádný DNS server, v sobě nemá odpověď na všechny otázky, které mu mohou být položeny. Hierarchická struktura jména, kdy jednotlivé její části jsou oddělené tečkou s pravidlem, že vyšší úroveň je vždy umístěna v adrese vpravo, umožňuje dohledat správnou cestu ke jmennému serveru, který je pro konkrétní adresu tzv. autoritativní (tj. má právo na podávání ověřených informací za určitou adresu). Každý z nich je totiž autoritativní pouze pro omezenou množinu adres.



Hrubý nákres struktury je vidět na Obrázku. Nejvyšší úroveň, tj. konec doménové adresy, je zde označen jako „.“. V další úrovni se vyskytují domény nejvyššího řádu a níže pak další úrovně jejich poddomén. Každá poddoména je sama o sobě doménou, která se může (a nemusí) dělit na další poddomény. Vzhledem k návrhu struktury DNS je možné správu DNS záznamů pro libovolnou z poddomén přidělit dalšímu jmennému serveru, který může být ve správě jiné organizace, čímž se v DNS dosahuje požadované decentralizovanosti.

## Root servery .

Kořenové jmenné servery (root name servers) představují zásadní část technické infrastruktury Internetu, na které závisí spolehlivost, správnost a bezpečnost operací na internetu. Tyto servery poskytují kořenový zónový soubor (root zone file) ostatním DNS serverům. Jsou součástí DNS, celosvětově distribuované databáze, která slouží k překladu unikátních doménových jmen na ostatní identifikátory.

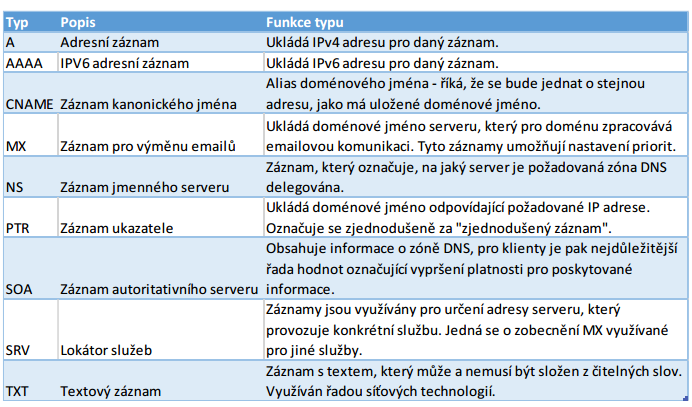
Kořenový zónový soubor popisuje, kde se nacházejí autoritativní servery pro domény nejvyšší úrovně. Tento kořenový zónový soubor je relativně velmi malý a často se nemění – operátoři root serverů ho pouze zpřístupňují, samotný soubor je vytvářen a měněn organizací [IANA](http://www.iana.org/).

## https://upload.wikimedia.org/wikipedia/commons/9/98/Dns-wikipedia.pngHledání IP adresy k doméně www.wikipedia.org

1. Uživatel zadal do svého [WWW klienta](https://cs.wikipedia.org/wiki/Webov%C3%BD_prohl%C3%AD%C5%BEe%C4%8D) doménové jméno www.wikipedia.org. Resolver v počítači se obrátil na lokální DNS server s dotazem na IP adresu pro www.wikipedia.org.
2. Lokální DNS server tuto informaci nezná. Má však k dispozici adresy kořenových serverů. Na jeden z nich se obrátí (řekněme na 193.0.14.129) a dotaz mu přepošle.
3. Kořenový server také nezná odpověď. Ví však, že existuje doména nejvyšší úrovně org, a jaké jsou její autoritativní servery, jejichž adresy tazateli poskytne.
4. Lokální server jeden z nich vybere (řekněme, že zvolí tld1.ultradns.net s IP adresou 204.74.112.1) a pošle mu dotaz na IP adresu ke jménu www.wikipedia.org.
5. Oslovený server informaci opět nezná, ale poskytne IP adresy autoritativních serverů pro doménu wikipedia.org. Jsou to ns0.wikimedia.org (207.142.131.207), ns1.wikimedia.org (211.115.107.190) a ns2.wikimedia.org(145.97.39.158).
6. Lokální server opět jeden z nich vybere a pošle mu dotaz na IP adresu ke jménu www.wikipedia.org.
7. Jelikož toto jméno se již nachází v doméně wikipedia.org, dostane od jejího serveru nepochybně autoritativní odpověď, že hledaná IP adresa zní 145.97.39.155
8. Lokální DNS server tuto odpověď předá uživatelskému počítači, který se na ni ptal.

# DNS Záznamy

Pro přenos DNS dat po síti se využívá formátu záznamů, který je označován jako Resource Record. Jednotlivé záznamy v sobě, kromě jiného, obsahují typ záznamu (Qtype) a každý z typů v sobě nese odlišné informace, jejichž přehled je v Tabulce.



# DNS Zóny

## Lookup Zone

Pro správu Microsoft DNS služby slouží snap-in do MMC konzole. V této konzoli se připojíme k určitému DNS serveru a ve stromu pod ním se nachází několik položek.

* *Cached Lookups* – každý DNS server standardně uchovává po určitou dobu záznamy, které v poslední době hledal, aby opakovaný dotaz mohl rychleji zodpovědět (pro zobrazení těchto záznamů musíme mít zapnuto Advanced View)
* *Forward Lookup Zones* – teprve zde jsou jednotlivé zóny (může jich být na serveru více), obsahuje mapování jmen na IP
* *Revers Lookup Zones* – obsahuje obrácené mapování IP adres na jména (PTR záznamy)