**18. Služby DNS, DHCP**

**1. Obecná charakteristika služeb DNS a DHCP**

**1.1 DNS (Domain Name System)**

* **Účel:** DNS slouží k překladu lidsky čitelných doménových jmen (např. [www.example.com](http://www.example.com/)) na IP adresy (např. 192.0.2.1), které jsou potřebné pro směrování síťového provozu.
* **Funkce:**
  + Distribuovaná databáze, která zajišťuje rychlé vyhledávání a resoluci názvů.
  + Hierarchická struktura domén (kořenová zóna, top-level domény, subdomény).
  + Podpora záznamů jako A (IPv4), AAAA (IPv6), CNAME, MX (mail exchange), NS (name server) a dalších.
* **Význam:** Umožňuje správné směrování provozu, zvyšuje efektivitu a usnadňuje správu sítě, zejména v rozsáhlých a dynamických prostředích.

**1.2 DHCP (Dynamic Host Configuration Protocol)**

* **Účel:** DHCP automatizuje proces přiřazování IP adres a dalších síťových parametrů (např. maska podsítě, výchozí brána, DNS servery) klientským zařízením.
* **Funkce:**
  + Dynamické přidělování IP adres na základě předdefinovaných rozsahů (poolů).
  + Obnova a uvolňování adres (leasing mechanismus).
  + Možnost konfigurace volitelných parametrů, jako jsou doménové jméno, WINS server apod.
* **Význam:** Snižuje administrativní zátěž spojenou s ruční konfigurací síťových nastavení a umožňuje snadné škálování sítě.

**2. Konfigurace a správa služby DNS**

**2.1 V OS Windows**

* **Nástroje a rozhraní:**
  + **DNS Manager:** Grafická konzole (součást nástrojů Windows Server), která umožňuje vytváření, úpravu a správu zón a záznamů.
  + **Příkazový řádek:** Nástroje jako nslookup pro testování resoluce, a PowerShell cmdlety (např. Add-DnsServerResourceRecordA, Get-DnsServerZone) pro automatizovanou správu.
* **Konfigurace:**
  + **Vytvoření DNS zóny:** Administrátor může vytvořit primární, sekundární nebo sub zónu. Primární zóna je místem, kde se uchovávají originální kopie záznamů.
  + **Nastavení replikace:** V doménovém prostředí se DNS záznamy replikují mezi řadiči domény (integrace s Active Directory).
  + **Konfigurace záznamů:** Přidávání záznamů typu A, AAAA, CNAME, MX, NS, PTR a dalších dle potřeb sítě**.**
  + **Zabezpečení:** Možnost nastavení dynamického aktualizování DNS záznamů a integrace s AD pro zvýšení bezpečnosti.

**2.2 V UNIX-like OS**

* **Nástroje a rozhraní:**
  + **BIND (Berkeley Internet Name Domain):** Nejrozšířenější DNS server pro UNIX-like systémy. Konfigurace probíhá pomocí textových konfiguračních souborů, typicky /etc/named.conf nebo /etc/bind/named.conf.
  + **Další alternativy:** Například dnsmasq nebo PowerDNS, které se mohou používat pro menší až středně velké sítě.
  + **Testovací nástroje:** Příkaz dig nebo nslookup pro ověření správné konfigurace a resoluce DNS záznamů**.**
* **Konfigurace:**
  + **Nastavení zón:** Definice zón a jejich typů (master, slave, forward) v konfiguračních souborech. Záznamy jsou specifikovány ve zvláštních souborech (např. /var/named/example.com.zone).??????????
  + **Replikace a sekundární servery:** Konfigurace slave zón, kdy sekundární servery automaticky synchronizují záznamy z primárního serveru.
  + **Bezpečnost:** Omezování přístupu k serveru, DNSSEC pro zabezpečení integrity dat a omezení dynamických aktualizací podle IP adres klientů.

**Konfigurace DNS serveru — /etc/bind/named.conf.options**

options {

listen-on port 53 { 127.0.0.1; 192.168.0.18; };

allow-query { localhost; 192.168.0.0/24; };

recursion yes;

forwarders {

8.8.8.8;

8.8.4.4;

};

}

**Konfigurace seznamu zón — /etc/bind/named.conf.local**

zone "firma.com" {

type master;

file "/etc/bind/db.firma.com";

};

zone "0.168.192.in-addr.arpa" {

type master;

file "/etc/bind/db.0.168.192.in-addr.arpa";

};

**Konfigurace jedné zóny — např. /etc/bind/db.firma.com**

; BIND db file for pepa.io

$TTL 86400

@ IN SOA ns.pepa.io. hostmaster.example.com. (

2024010401 ; serial number YYMMDDNN

28800 ; Refresh

7200 ; Retry

864000 ; Expire

86400 ; Min TTL

)

NS ns.pepa.io.

$ORIGIN pepa.io.

ns A 10.4.20.1

ns A 10.0.50.1

www A 10.0.50.2

router CNAME ns

server CNAME www

**3. Konfigurace a správa služby DHCP**

**3.1 V OS Windows**

* **Nástroje a rozhraní:**
  + **DHCP Manager:** Grafická konzole pro konfiguraci a správu DHCP serveru, která je součástí Windows Server**.**
  + **Příkazový řádek a PowerShell:** Cmdlety jako Add-DhcpServerv4Scope, Set-DhcpServerv4OptionValue umožňují skriptovanou správu.
* **Konfigurace:**
  + **Vytvoření DHCP rozsahu (scope):** Definování rozsahu IP adres, které může server dynamicky přidělovat, spolu s nastavením rezervací a výluk.
  + **Nastavení volitelných parametrů:** Konfigurace volitelných DHCP parametrů jako maska podsítě, výchozí brána, DNS servery, doménové jméno apod.
  + **Zabezpečení a autorizace:** DHCP server je autorizován v Active Directory, což zabraňuje spouštění neautorizovaných serverů ve stejné síti.
  + **Rezervace a statické adresy:** Administrátor může vytvořit rezervace pro specifická zařízení na základě MAC adresy, aby získávala vždy stejnou IP adresu.

**3.2 V UNIX-like OS**

* **Nástroje a rozhraní:**
  + **ISC DHCP Server:** Jeden z nejpoužívanějších DHCP serverů v Linuxu. Konfigurace probíhá v textovém souboru (typicky **/etc/dhcp/dhcpd.conf**).
  + **Alternativní řešení:** Například dnsmasq, který může fungovat jako lehký DHCP server i DNS cache**.**
  + **Testovací nástroje:** Příkazy jako dhcpdump pro analýzu provozu DHCP, logování a sledování přidělených adres.
* **Konfigurace:**
  + **Definování rozsahu a možností:** V konfiguračním souboru se nastaví rozsah IP adres (pool), časová prodleva (lease time) a další volitelné parametry jako směrovač (router), DNS servery a další.
  + **Rezervace a statické přidělení:** Možnost konfigurace rezervací pro specifické klienty na základě jejich MAC adresy.
  + **Integrace a replikace:** V rámci větších sítí lze implementovat redundantní DHCP servery, kde jeden server slouží jako primární a druhý jako záložní pro nepřetržitý provoz.

# Konfigurace globálních parametrů (v dhcpd.conf)

option domain-name "pepa.io";

option domain-name-servers 10.4.20.1, 10.0.50.1;

default-lease-time 600;

max-lease-time 7200;

ddns-update-style none;

# Konfigurace podsítě

subnet 10.0.50.0 netmask 255.255.255.0 {

# Lze sem nakonfigurovat lokální parametry pro tu danou podsíť

# option routers 10.0.50.1;

}

subnet 10.4.20.0 netmask 255.255.255.0 {

range 10.4.20.69 10.4.20.88;

option routers 10.4.20.1;

}

# Můžeme zde i nakonfigurovat hosty

# kterým budou podle MAC adresy staticky

# přiřazeny IP adresy

host server {

hardware ethernet 08:00:27:b2:30:11;

fixed-address 10.0.50.2;

option routers 10.0.50.1;

}

**Shrnutí**

* **DNS:**
  + Zajišťuje překlad doménových jmen na IP adresy a funguje jako distribuovaná hierarchická databáze.
  + Ve Windows se spravuje pomocí DNS Manageru a BCD, zatímco v UNIX-like OS je standardem BIND (nebo alternativy jako dnsmasq).
  + Konfigurace zahrnuje nastavení zón, záznamů (A, AAAA, CNAME, MX, NS, PTR) a zabezpečení pomocí DNSSEC či omezení dynamických aktualizací.
* **DHCP:**
  + Automatizuje přiřazování IP adres a síťových parametrů klientským zařízením, čímž zjednodušuje správu sítě.
  + Ve Windows se využívá DHCP Manager a PowerShell, zatímco v UNIX-like OS se často používá ISC DHCP server nebo dnsmasq.
  + Klíčová konfigurace zahrnuje definování rozsahu IP adres, rezervací, nastavení volitelných parametrů a zabezpečení (např. autorizace serveru v AD).