# 17 — Doménový systém

- **DNS** (Domain Name System) je hierarchický systém doménových jmen, který je realizován **servery DNS** a **protokolem stejného jména**, kterým si vyměňují informace.
- **hlavním úkolem:** jsou vzájemné převody doménových jmen a IP adres uzlů sítě.
- **další funkce:** např. pro elektronickou poštu

**Motivace - proč DNS?**
V dnešních sítích se převážně používá adresovaní na bázi IP adres. Tyto jsou obtížně zapamatovatelné a s příchodem IPv6 je zapamatování adresy nemyslitelné. Proto se začal vytvářet soubor HOSTS ( ve světě UN*Xu zpravidla /etc/hosts ), který obsahoval jednoduchou "databázi" názvů strojů a IP adres ve formatu IPadresa FQDN hostname. Toto řesení samozřejmě nemohlo plnohodnotne fungovat, protože databáze se musela často aktualizovat a distribuovat mezi kazdý stroj, což bylo velmi náročné na kapacitu sítě a úsilí správců. Velký rozvoj Internetu a sití obecně si vyžádal vyřešení tohoto problému, čímž byl systém DNS.

**Jak to funguje?**
Systém DNS je celosvětová distribuovaná databáze umožnující přeložit adresu v doménovém tvaru na odpovídající IP adresu a doručování pošty. Princip fugování je následující: klient se zeptá na překlad primárního DNS serveru pro sít v níž je připojen( pokud ten není dostupný, tak sekundárního, dalsího sekundárního...), a ten pokud má v záznamech tak údaj poskytne a pod ne, tak se sám zeptá jiného serveru, který je v hierarchii DNS výše, ten se může také zeptat výše, atd. Nejvýše se dotaz může dostat k ROOT-DNS serveru. ( Těchto serverů je na světě 13 a tvoří kořen hierarchie DNS. ) Při spravne odpovedi od nadřazeného serveru si kazdy server muze kešovat informace, ktere poskytuje klientum, cím se urychlí dalsí dotazy. Doba, po jakou se muze informace kešovat je jednoznačne dána v konfiruraci serveru, ktery odpovedel. Nastavení klienta v linuxu(resolveru) je uloženo v souboru /etc/resolv.conf.

**Bezpečnost**
Zakladem bezpecnosti je NEMÍT server bežící se superuživatelskými právy. Dalším stupněm bezpečnosti je tzv. Chrootovane prostředí. Jedna se o změněný root adresář, takže pokud dojde k ovládnutí procesu DNS serveru, pak ovládnutí celého stroje je složitejší a náročnější na útočníka. Základem je vytvoření adresáře např. /chroot do kterého nakopírujeme soubory potřebné k běhu bindu a to tak, že respektujeme cesty např. /etc/named.conf nakopírujeme do /chroot/etc/named.conf. Dále je potřeba nakopírovat knihovny nutné pro běh programu ( zjistíme ldconfig -r /chroot/named ), musíme také vytvořit zařízení /chroot/dev/null. Běh bindu v chrootovaném prostředí nemůže zabránit všem bezpecnostním problémům, nicméně omezí rizika na minimum. Skutečností je, že většina útoků na www je realizována změnou dns záznamů.