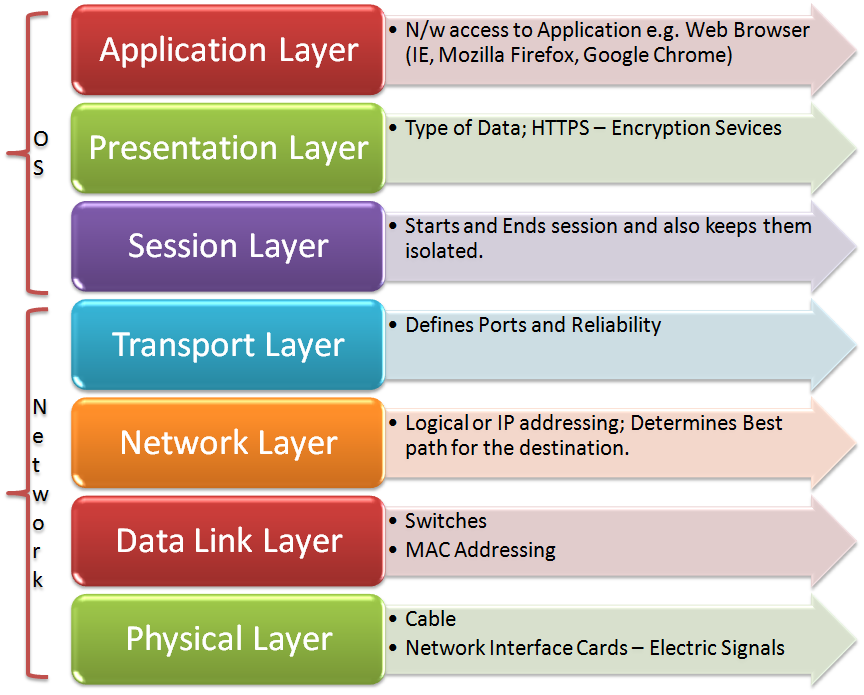
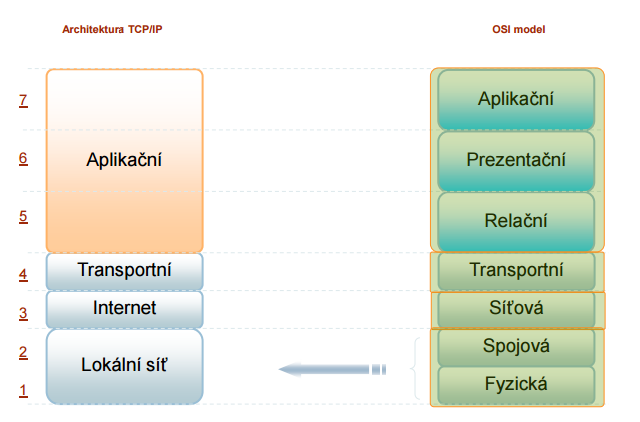
PSI

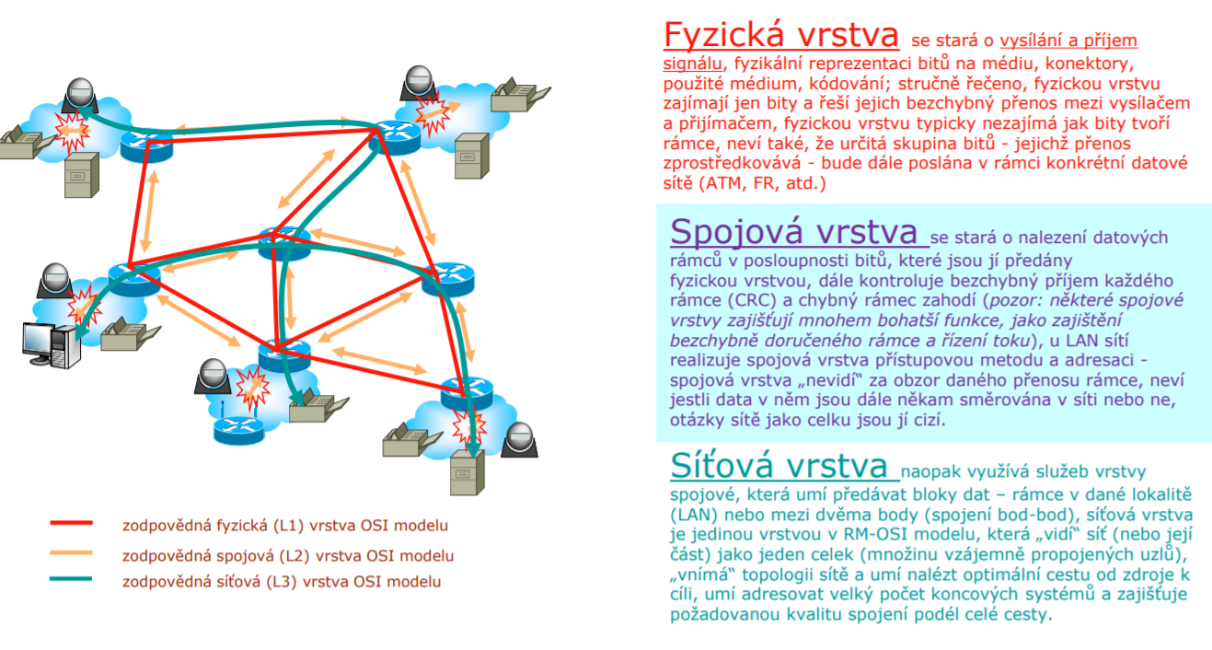
Model OSI, přístupy k přenosovému médiu, síťová vrstva, komunikační protokoly, bezpečnost sítí, datová kvalita, správa sítí. (PSI)

# Model OSI

* Referenční model ISO/OSI vypracovala organizace ISO jako hlavní část snahy o standardizaci počítačových sítí.
* Úlohou referenčního modelu je poskytnout základnu pro vypracování norem pro účely propojování systémů. Norma tedy nespecifikuje implementaci systémů, ale uvádí všeobecné principy sedmivrstvé síťové architektury. Popisuje vrstvy, jejich funkce a služby.
* Nejsou zde zařazeny žádné protokoly, které by vyžadovaly zbytečně mnoho detailů.
* Reálně je vrstvený model použit například u rodiny protokolů [TCP/IP](https://cs.wikipedia.org/wiki/TCP/IP), kde jsou však použity jen čtyři vrstvy.

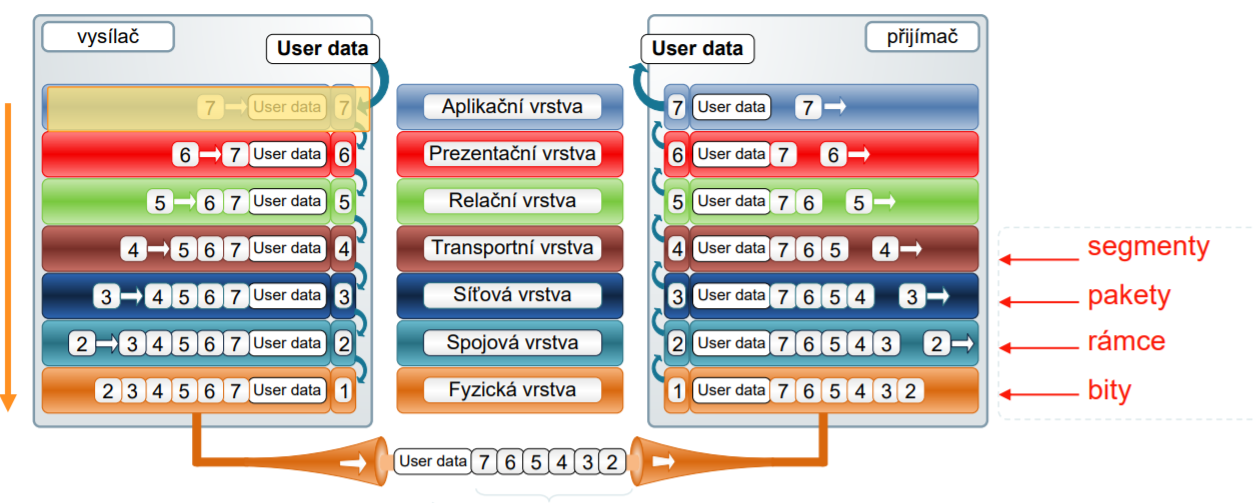


* **Fyzická**: umožňuje přenos bitů kanálem, definuje „0“ a „1“, předepisuje vlastnosti média, definuje elektrické a mechanické vlastnosti rozhraní
* **Spojová:** funkce spolehlivého spojení (detekce a korekce chyb), formátování dat do rámců, rozpoznávání rámců, řízení toku na lince, jednoznačnou adresu v rámci segmentu (MAC)
* **Síťová:** adresaci a směrování dat přes mezilehlé prvky, jednoznačnou adresu v rámci sítě (IP), nalezení optimální cesty v síti, kvalitu trasy, fragmentace paketů
* **Transportní:** rozklad dat na segmenty, uspořádání dat podle pořadí, koncové řízení toku, TCP, UDP
* **Relační:** vytváření logického rozhraní pro aplikace, synchronizace spojení (transakce).
* **Prezentační:** dohodu o syntaxi, šifrování, kompresi.
* **Aplikační:** knihovny pro tvorbu síťových aplikací.



## Princip zapouzdření vrstev – vrstevnatost

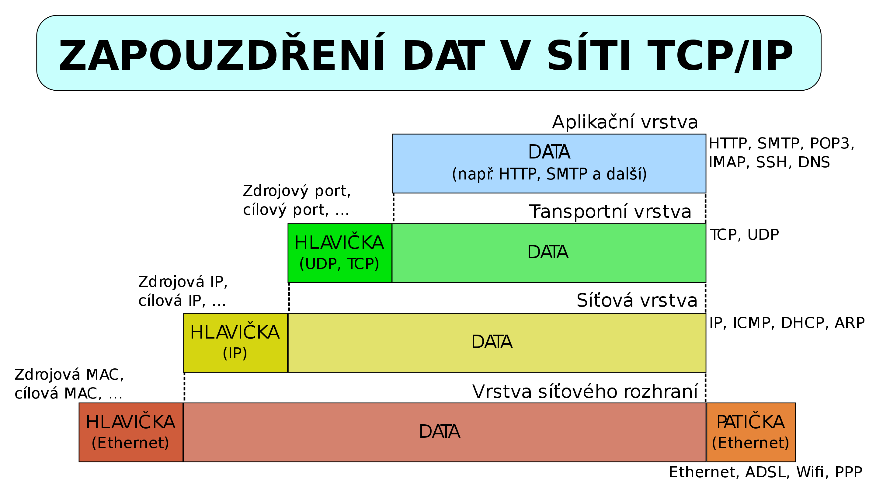
* Každá ze sedmi vrstev vykonává skupinu jasně definovaných funkcí potřebných pro komunikaci. Pro svou činnost využívá služeb své sousední nižší vrstvy. Své služby pak poskytuje sousední vyšší vrstvě.
* Současně se při přechodu z vyšší vrstvy k nižší přidávají k uživatelským (aplikačním) datům záhlaví jednotlivých vrstev. Tak dochází k postupnému zapouzdřování původní informace. U příjemce se postupně zpracovávají řídící informace jednotlivých vrstev a vykonávají jejich funkce.



* Efektivita je poměr celkového počtu přenášených a aplikačních dat
* Vyjádřeno v procentech:

# TCP IP

* Rodina protokolů TCP/IP obsahuje sadu protokolů pro komunikaci v počítačové síti a je hlavním protokolem celosvětové sítě Internet.
* Komunikační protokol je množina pravidel, která určují syntaxi a význam jednotlivých zpráv při komunikaci.
* Architektura TCP/IP je členěna do čtyř vrstev (na rozdíl od referenčního modelu OSI se 7):
* **Aplikační vrstva** (application layer)
* **Transportní vrstva** (transport layer)
* **Síťová vrstva** (internet layer)
* **Vrstva síťového rozhraní** (network interface)

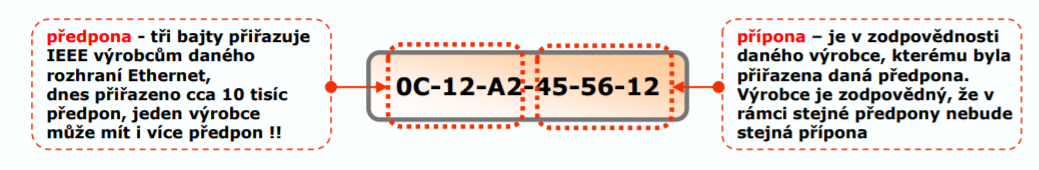


## Vrstva síťového rozhraní – Ethernet, WiFi, Bluetooth…

* Nejnižší vrstva umožňuje přístup k fyzickému přenosovému médiu. Je specifická pro každou síť v závislosti na její implementaci. Příklady sítí: Ethernet, WiFi …
* Specifikuje fyzickou komunikaci. Aktivuje, udržuje a deaktivuje fyzické spoje (např. komutovaný spoj) mezi koncovými systémy. Fyzické spojení může být dvoubodové (sériová linka) nebo mnohobodové (Ethernet).
* Fyzická vrstva definuje všechny elektrické a fyzikální vlastnosti zařízení.
* Hlavní funkce poskytované fyzickou vrstvou jsou:
  + Navazování a ukončování spojení s komunikačním médiem.
  + Spolupráce na efektivním rozložení všech zdrojů mezi všechny uživatele.
  + Modulace neboli konverze digitálních dat na signály používané přenosovým médiem

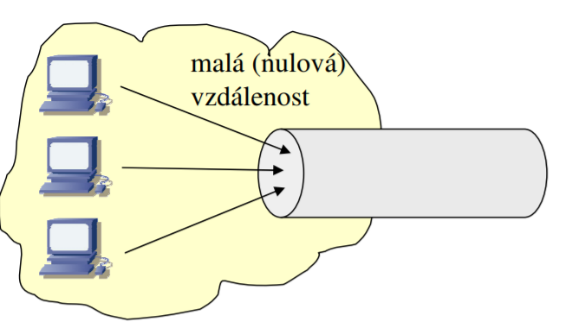
### MAC

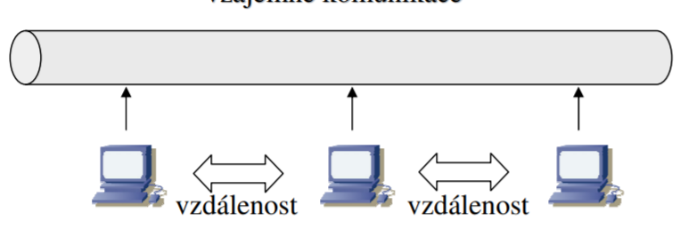
* MAC adresa Je přiřazována síťové kartě bezprostředně při její výrobě, a proto se jí také někdy říká fyzická adresa
* Ethernetová MAC adresa se skládá ze 48 bitů a podle standardu by se měla zapisovat jako šestice dvojciferných hexadecimálních čísel
* oddělených pomlčkami (např. 01-23-45-67-89-ab)
* Původní standard MAC adresy přidělené výrobcem předpokládal, že adresa bude vždy celosvětově jedinečná.
* V případě, že se v lokální síti poté objeví dvě zařízení, která mají stejnou MAC adresu, je tato kolize obvykle řešena virtuální změnou (u moderních karet). Pravděpodobnost této kolize je však velice nízká a projevuje se obvykle až u velkých lokálních sítí.

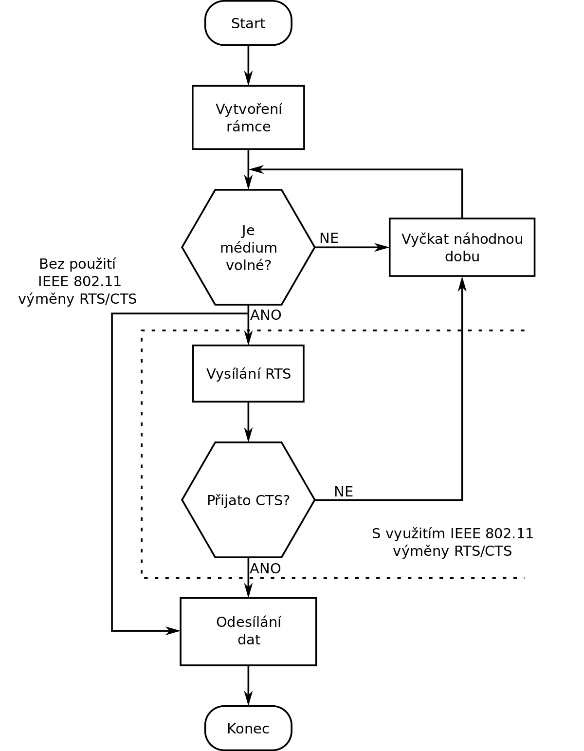


### Sdílený přístup k mediu

Současné vysílání více uzlů vede ke kolizi rámců. Více vysílání navzájem interferuje, takže jsou všechny zkresleny a přijímače nejsou schopny rozlišit překrývající se přijaté signály jeden od druhého.

**Multiplexování**: je v elektronice, telekomunikacích a počítačových sítích termín popisující proces, ve kterém je více analogových signálů nebo digitálních datových toků kombinováno do jednoho signálu. Cílem je co možná nejefektivnější využití daného přenosového média.

**Přístupová metoda**: Zařízení se chce odeslat data do kanálu, kde již probíhá komunikace



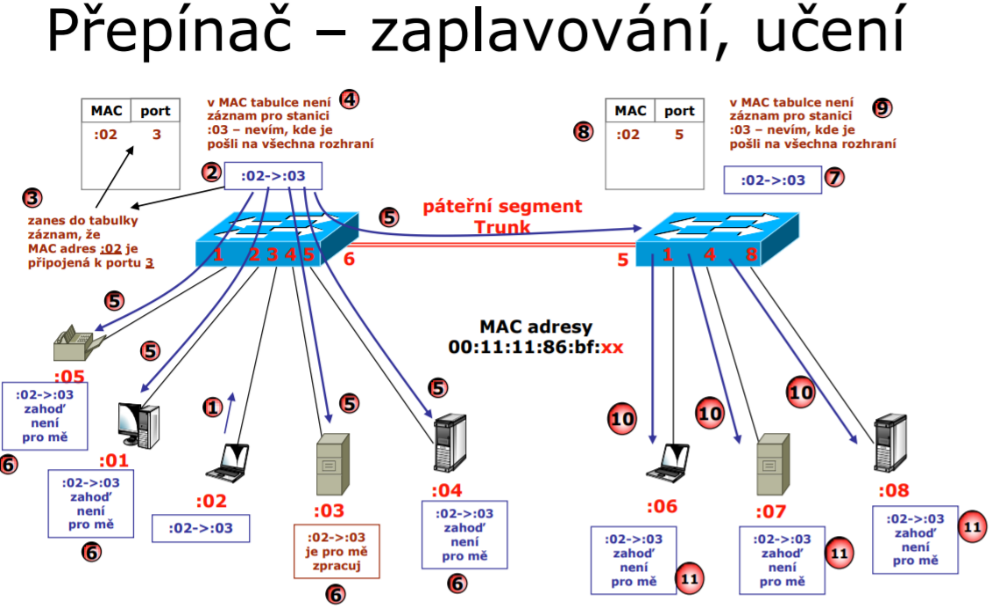
#### WIFI – CSMA/CA:

* V sítích CSMA je nemožné zcela zabránit kolizím, avšak existují způsoby, jak se s nimi vypořádat.
* je pravděpodobnostní protokol přístupu k médiu, ve kterém uzel ověřuje nepřítomnost dalšího provozu před vysíláním na sdíleném fyzickém médiu, jako například elektrickém propojovacím vedení či pásmu elektromagnetického spektra.

#### Ethernet – Plný duplex:

* Díky masivnímu rozšíření přepínačů je dnes obvyklé, že koncový počítač je přímo propojen s přepínačem. [Kolizní doména](https://cs.wikipedia.org/wiki/Kolizn%C3%AD_dom%C3%A9na) tudíž obsahuje jen dva účastníky
* Provoz kabelem může protékat obousměrně (více párů kabelů), každý z účastníků má své pevně přidělené vodiče, do nichž může vysílat kdykoli. Odpadá sdílení média a s ním i důvody pro nasazení algoritmu CSMA/CD.
* Odpadají v něm prostoje způsobené kolizemi a přenosová rychlost odpovídá maximální možné.

### Přepínač

* Síťový přepínač (anglicky switch) je v informatice aktivní prvek v počítačové síti, který propojuje jednotlivé prvky do hvězdicové topologie. Přepínač obsahuje větší či menší množství síťových portů (až několik stovek), na něž se připojují síťová zařízení nebo části sítě. Přepínač přeposílá síťový provoz jenom do těch smě
* Adresování se přepínači učí automaticky z procházejícího provozu, konkrétně z adres odesilatelů uvedených v rámcích, které do přepínače přicházejí. Používá se algoritmus Backward Learning Algorithm
* Přepínač si podle příchozích rámců mapuje porty na mac adresy
* Pokud přepínač dostane k doručení rámec směřující na jemu dosud neznámou adresu, chová se jako hub a rozešle rámec do všech ostatních rozhraní. Lze očekávat, že oslovená stanice pravděpodobně odpoví a přepínač se tak vzápětí dozví, kde se nachází. 

#### Topologie – Spanning Tree Protocol

Ethernetové přepínače mají problém se smyčkami v síti. Pokud síť obsahuje smyčku (mezi dvěma uzly existuje více než jedna cesta), mohou pakety od stejného odesilatele přicházet chaoticky z různých rozhraní, a dokonce tentýž paket může do přepínače dorazit několikrát. Přepínač není v takovém prostředí schopen rozpoznat, kde se kdo nachází.

Tento problém řeší přepínače mechanismem zvaným Spanning Tree Protocol, kterým se dohodnou na nepoužívání některých tras tak, aby ze sítě zmizely smyčky. Vytvoří se minimální kostra sítě dosahující do všech jejích míst. Když dojde ke změně v topologii, bude aktivována některá z dosud odstavených tras tak, aby nový strom nadále pokud možno pokrýval celou síť. Tyto změny se ovšem nedějí okamžitě, je zde jisté zpoždění.

## Síťová vrstva – Ipv4, IPv6, RIPv2, EIGRP, OSPF…

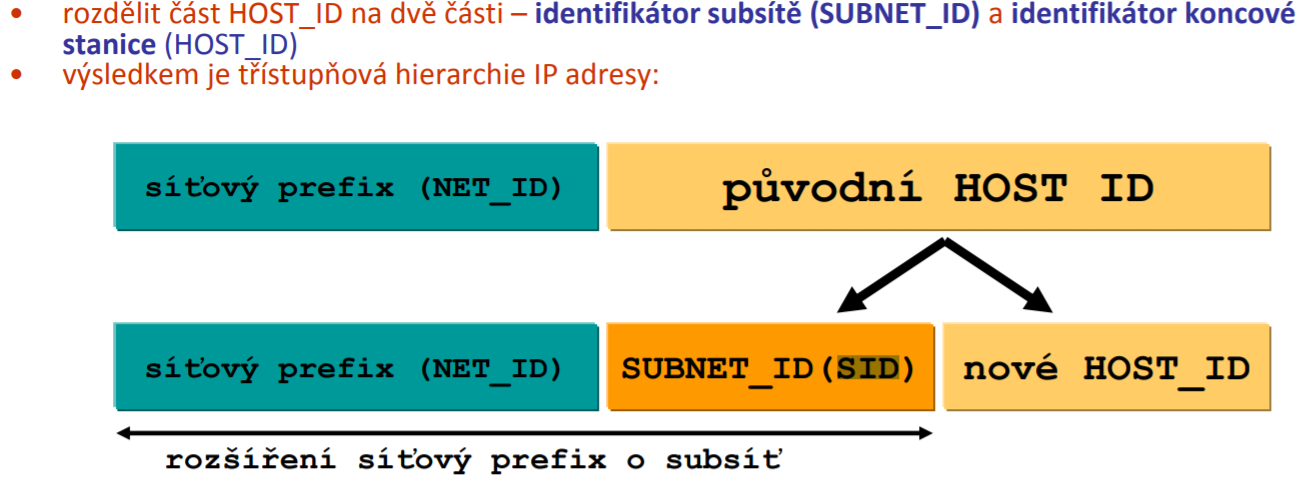
* Síťová vrstva (anglicky network layer) je v informatice název třetí vrstvy síťové architektury referenčního modelu ISO/OSI.
* Obsahuje funkce, které umožňují překlenout rozdílné vlastnosti technologií v přenosových sítích. Nejznámější protokol, který pracuje na této vrstvě je protokol Internet Protocol (IP).
* Internet Protocol je zodpovědný za směrování datagramů (paketů) ze zdrojového počítače do cílového hostitele přes jednu nebo více IP sítí.
* Data se v IP síti posílají po blocích nazývaných datagramy. Jednotlivé datagramy putují sítí zcela nezávisle, na začátku komunikace není potřeba navazovat spojení
* IP v doručování datagramů poskytuje nespolehlivou službu, označuje se také jako best effort – „nejlepší úsilí“; tj. všechny stroje na trase se datagram snaží podle svých možností poslat blíže k cíli, ale nezaručují prakticky nic.
* Na druhou stranu příležitostná chyba nemívá pozorovatelný efekt. Navíc se obvykle používá vyšší vrstva, která ji automaticky opraví.
* Návrh internetových protokolů předpokládá, že síťová infrastruktura je neodmyslitelně nespolehlivá a dynamická z hlediska dostupnosti a propojení uzlů. Neexistuje žádný centrální monitoring anebo měření výkonnosti, který by umožňoval sledování, nebo udržování stavu sítě.

### Formát IP v4 paketu

* Kontrolní součet IP hlavičky,
* TTL time to live Počet skoků jumps
* Celková délka přenášených dat
* Cílová / zdrojová IPv4 adresa

### IP adresy

* Z pohledu fyzického i logického pohledu nepoužíváme jednu globální síť, ale hierarchické dělení na různé části zvané subnety (podsítě)
* každá organizace si může svobodně rozdělit svůj přiřazený adresní prostor na různý počet interních směrovaných subsítí
* Vnitřně jsou subsítě brány jako odlišné IP sítě v rámci organizace
* Z vnějšího světa však subsítě nejsou viditelné, celá síť se chová jako jediný celek s jednou IP adresou sítě –> agregace adresového prostoru



* Maska vyjadřuje velikost, kolik bitů z IP adresy označuje síť a kolik jednotlivé zařízení



### Směřování – RIPv2, EIGRP, OSPF, BGP

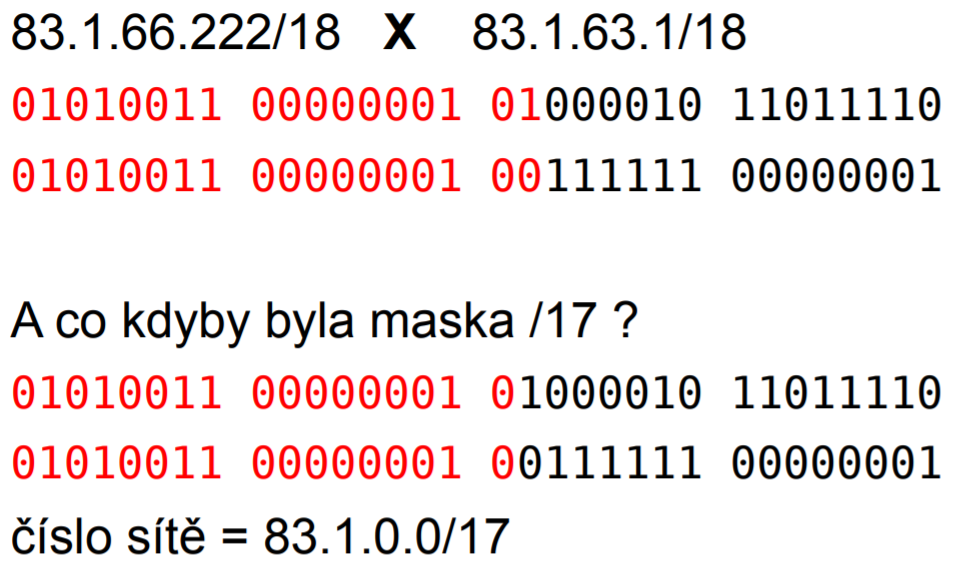
* Směruje podle adresy sítě, první část adresy rozdělné maskou
* Každé síťové rozhraní komunikující prostřednictvím IP má přiřazeno jednoznačný identifikátor, tzv. IP adresu. V každém datagramu je pak uvedena IP adresa odesílatele i příjemce. Na základě těchto adres pak směrovače (routery) na trase provádí rozhodnutí, jakým směrem paket odeslat, tzv. směrování (routing).
* Routery v přenosové cestě pouze přepošlou pakety na další známé místní brány, které odpovídají směrovacímu prefixu cílové adresy a jsou „blíže“ cílové adrese
* Vzhledem k tomu, že je směrování dynamické pro každý paket a síť si neuchovává stav cesty, je možné, že některé pakety jsou směrovány přes delší cestu k určenému cíli, což vede k nesprávnému pořadí v přijímači.
* směrovač nemusí mít nezbytně ve své směrovací tabulce záznamy o všech sítích existujících IP sítích (např. internet nebo podniková síť)
* stačí, když bude vědět, jak směrovat pakety jen k určité podmnožiny všech sítí
* všechny ostatní IP pakety, které nedokáže směrovač směrovat (není pro ně v tabulce relevantní záznam), pošle jinému směrovači, o němž se domnívá, že má více informací a že tedy dokáže IP pakety správně směrovat
* Jak se plní směrovací tabulky můžou být plněny manuálně nebo dynamicky

**Co je to směrovací metrika.**

* pokud v datové síti existuje od zdrojové stanice více alternativních cest k cílové stanice, je nutné podle dnešní představy fungování přenosu dat vybrat typicky jen jedinou (neuvažujeme nyní „loadbalancing“), po níž se budou pakety přenášet
* v praxi se každé cestě přiřadí kvantifikující číselná veličina, která se častěji nazývá jako metrika
* do výpočtu metriky lze zahrnout celou řadu kritérií, jako je **počet směrovačů** v cestě, výslednou **přenosová rychlost**, **zpoždění** průchodu paketu cestou, **aktuální zatížení cesty**, **spolehlivost**,

**Směřování v místních sítích**

* Jak koncové zařízení určí, zda zpracovávaný paket má být poslán lokálně v rámci LAN sítě přímo koncové stanici nebo přes směrovač.
  + Čísla sítě se musí shodovat.



* Vynásobení zdrojové IP lokální maskou = IPNetworkLocal
* Vynásobení cílové IP lokální maskou = IPNetworkDestination
* Jestliže se IPNL a IPND rovnají, je cílová stanice ve stejné síti jako já a pomocí ARP zjistí MAC adresu cílové IP stanice, když se nerovnají pošle lokálnímu směrovači – IP pakety zabalí do ethernet rámců se zdrojovou a cílovou MAC

## Transportní vrstva – TCP, UDP

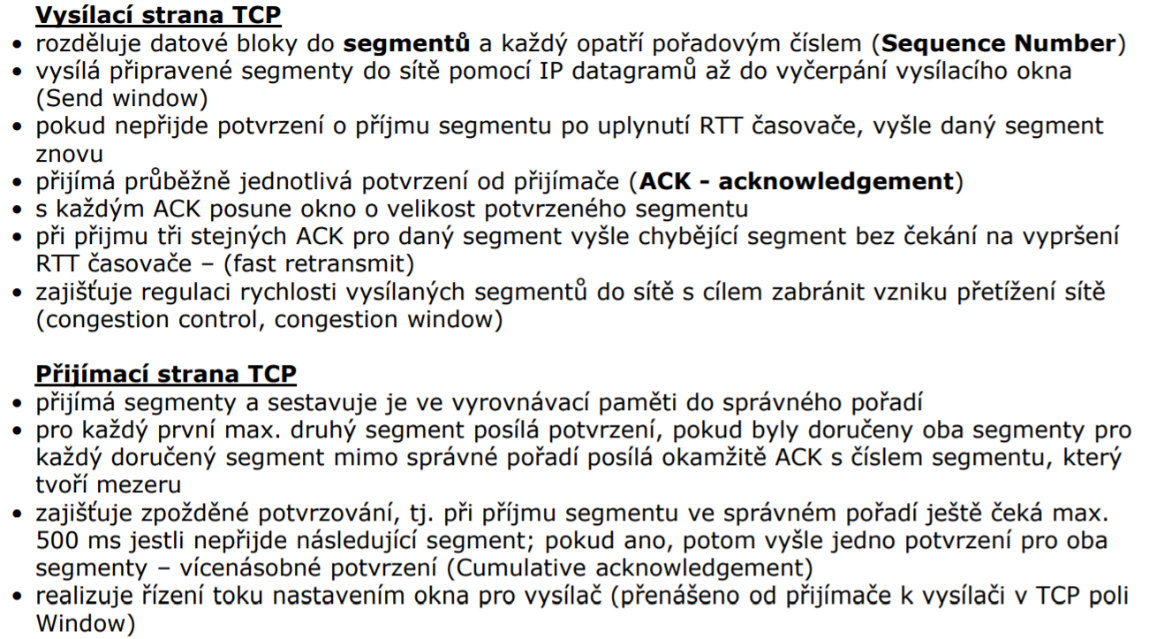
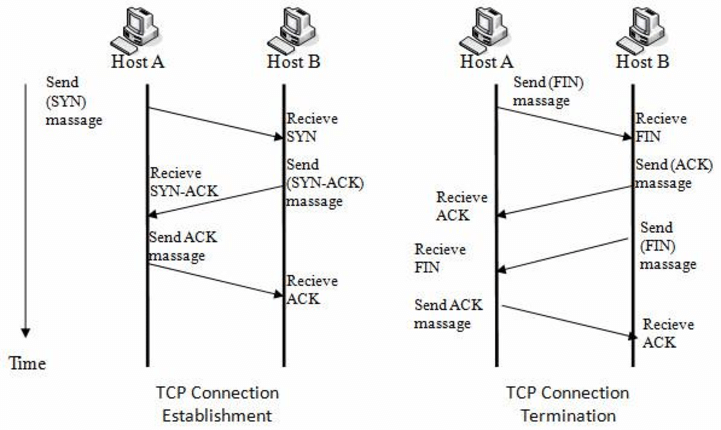
* Poskytuje transportní služby pro kontrolu celistvosti dat: kontrolované spojení spolehlivým protokolem TCP nebo nekontrolované spojení nespolehlivým protokolem UDP.
* Transportní vrstva je implementována až v koncových zařízeních (počítačích) a umožňuje proto přizpůsobit chování sítě potřebám aplikace.
* Doručení se zárukou / bez záruky znamená, zdali je nám zaručeno, že datové rámce, které vznikly fragmentací dat určených k přenosu, dorazí do cílové stanice všechny a ve stejném pořadí.

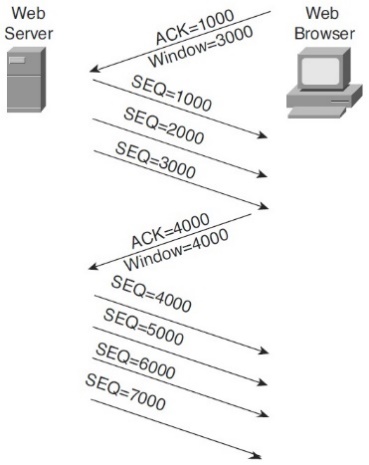
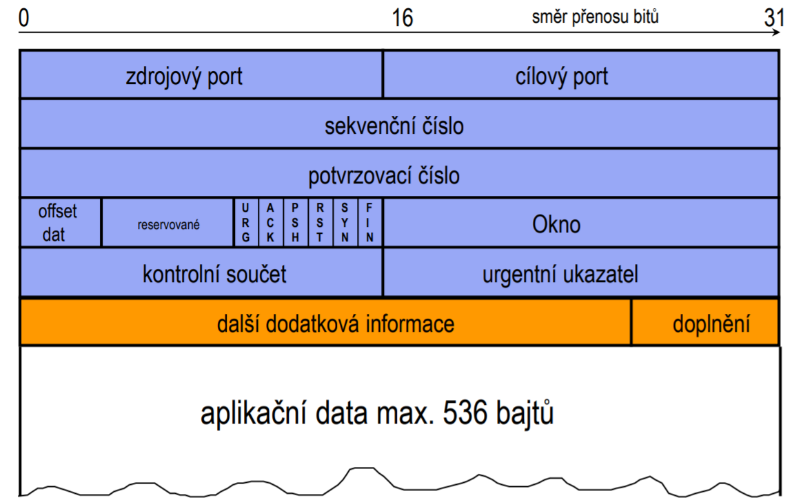
### UDP – nezaručuje přenos

Protokol UDP je vhodný pro nasazení, které vyžaduje jednoduchost, malá režie nebo pro aplikace pracující systémem otázka-odpověď (např. DNS, sdílení souborů v LAN).

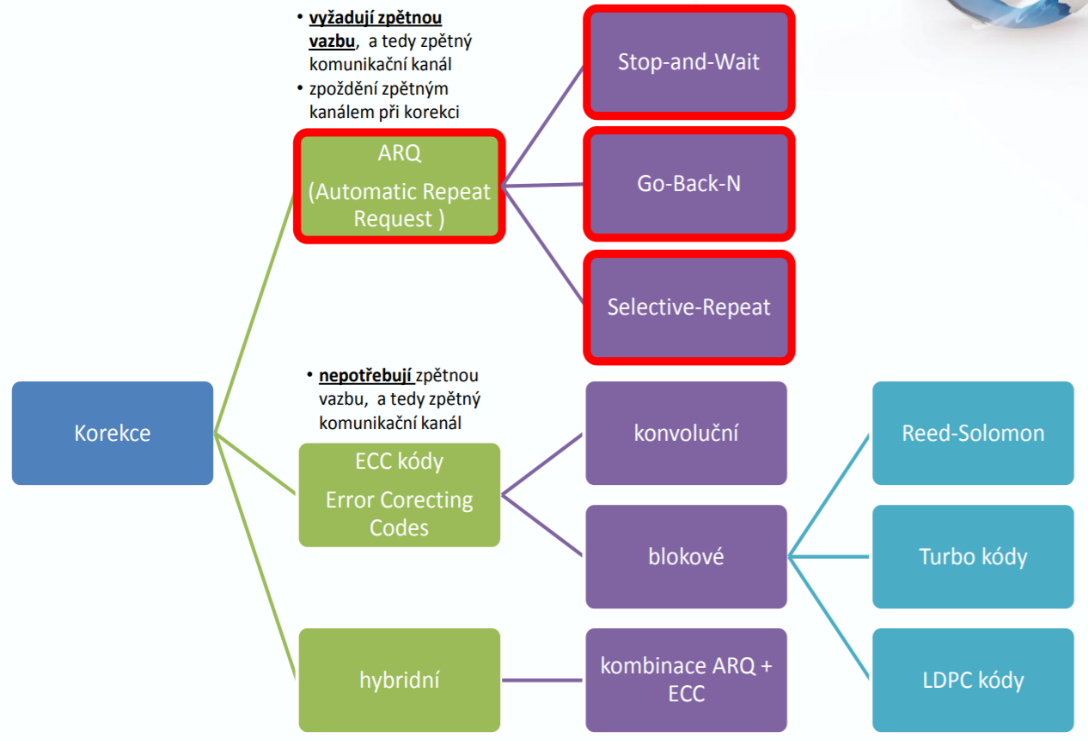
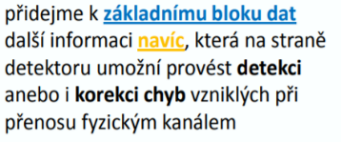
Jeho bezestavovost je užitečná pro servery, které obsluhují mnoho klientů nebo pro nasazení, kde se počítá se ztrátami datagramů a není vhodné, aby se ztrácel čas novým odesíláním (starých) nedoručených zpráv (např. VoIP, online hry).

### TCP – bezpečný přenos

Transmission Control Protocol (TCP) je nejpoužívanějším protokolem transportní vrstvy v sadě protokolů TCP/IP používaných v síti Internet. Použitím TCP mohou aplikace na počítačích propojených do sítě vytvořit mezi sebou spojení, přes které mohou obousměrně přenášet data. Protokol garantuje spolehlivé doručování a doručování ve správném pořadí. TCP také umožňuje rozlišovat a rozdělovat data pro více aplikací (například webový server a emailový server) běžících na stejném počítači.



#### Zajištění integrity dat a opravy chyb



#### Automatic repeat request

* souhrnný název pro různé metody detekce a korekce chyb používané při přenosu dat, které pro zajištění spolehlivého přenosu dat nespolehlivým kanálem používají kladná potvrzení a časové prodlevy.

**Princip klouzavého okna – Stop and wait**

* Odesílatel vždy vysálá několik paketů najednou a doufá, že se neztratí.
* Na začátku vyšle n paketů. Pokud mu přijde potvrzení odešle x paketů, kde x je rozdíl posledního odeslaného a právě přijatého, tak si v kanále udržuje n odeslaných paketů
* Zvýšení efektivity, jelikož nečeká na potvrzení každého paketu.

***GO-back-N***

* odesílající proces pokračuje v posílání dalších datových rámců až do počtu daného velikostí okénka, i když nepřijal potvrzení příjmu (ACK) od přijímající strany.
* Přijímající proces si pamatuje pořadové číslo dalšího rámce, jehož přijetí očekává, a toto číslo posílá v každém potvrzení. Přijímač zahodí každý rámec, jehož číslo se neshoduje s očekávaným pořadovým číslem, a opakuje vysílání potvrzení s číslem prvního očekávaného rámce
* Při detekci chyby se posílá celé okénko od posledního potvrzeného okna
* **Deadlock**: Pokud nastane timeout a odesílatel je nedostává použije tzv. Flooding, kdy pošle celý rámec najednou

***Selective repeat***

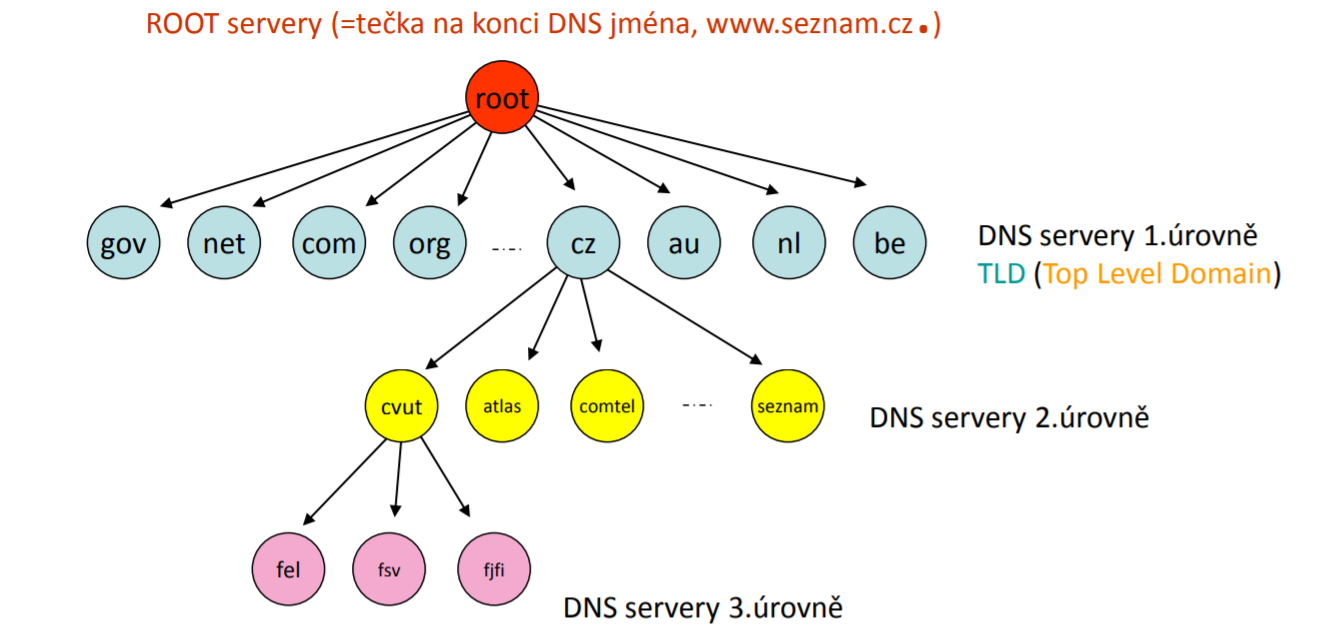
* odesílající proces pokračuje v posílání dalších datových rámců až do počtu daného velikostí okénka, i když nepřijal potvrzení příjmu (ACK) od přijímající strany.
* Příjemce informuje odesilatele, které rámce mu chybí, takže odesilatel může opakovat vysílání pouze chybějících rámců.
* Při selektivním opakování příjemce přijímá i rámce mimo pořadí a ukládá je. Odesilatel jednotlivě opakuje vysílání rámců, u kterých vypršela prodleva pro potvrzení.
* **Lepší**: při detekci chyby je požadován pouze ztracený paket, jelikož možné další pakety jsou zakešované.

# Fungování internetu jako celku

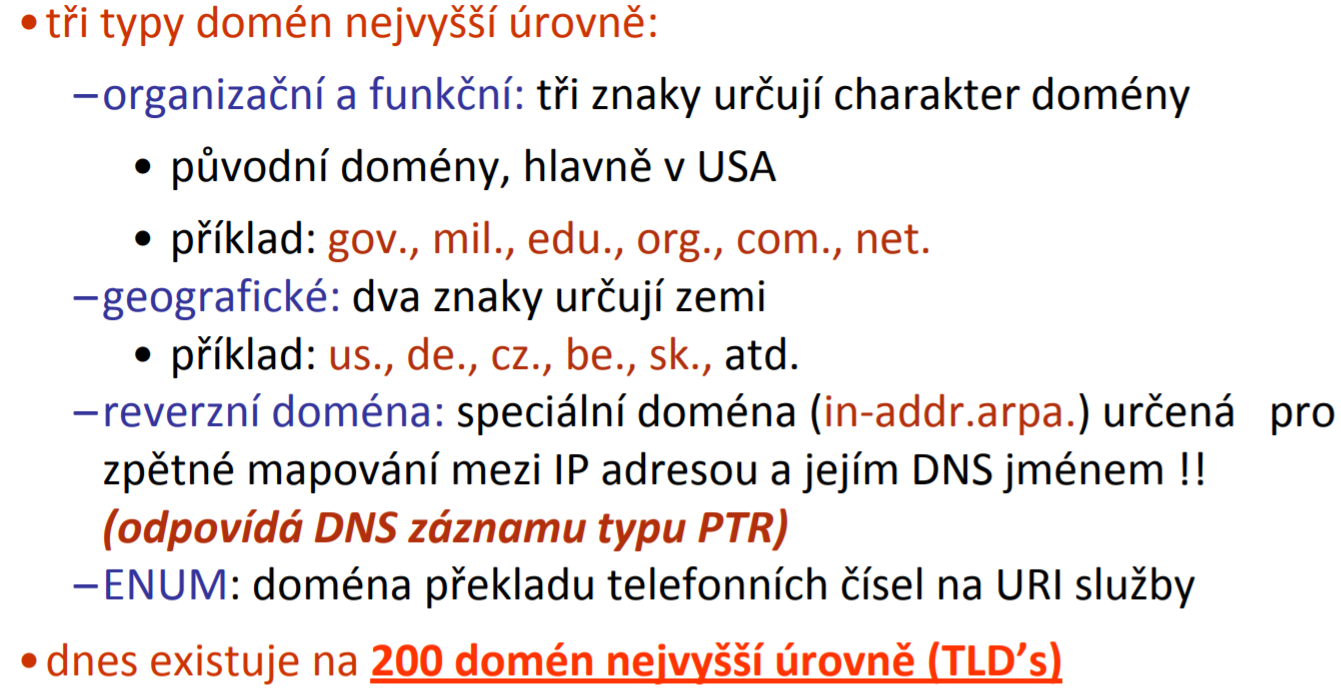
## DNS

DNS (Domain Name System) je hierarchický, decentralizovaný systém doménových jmen, 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 uzlů sítě.

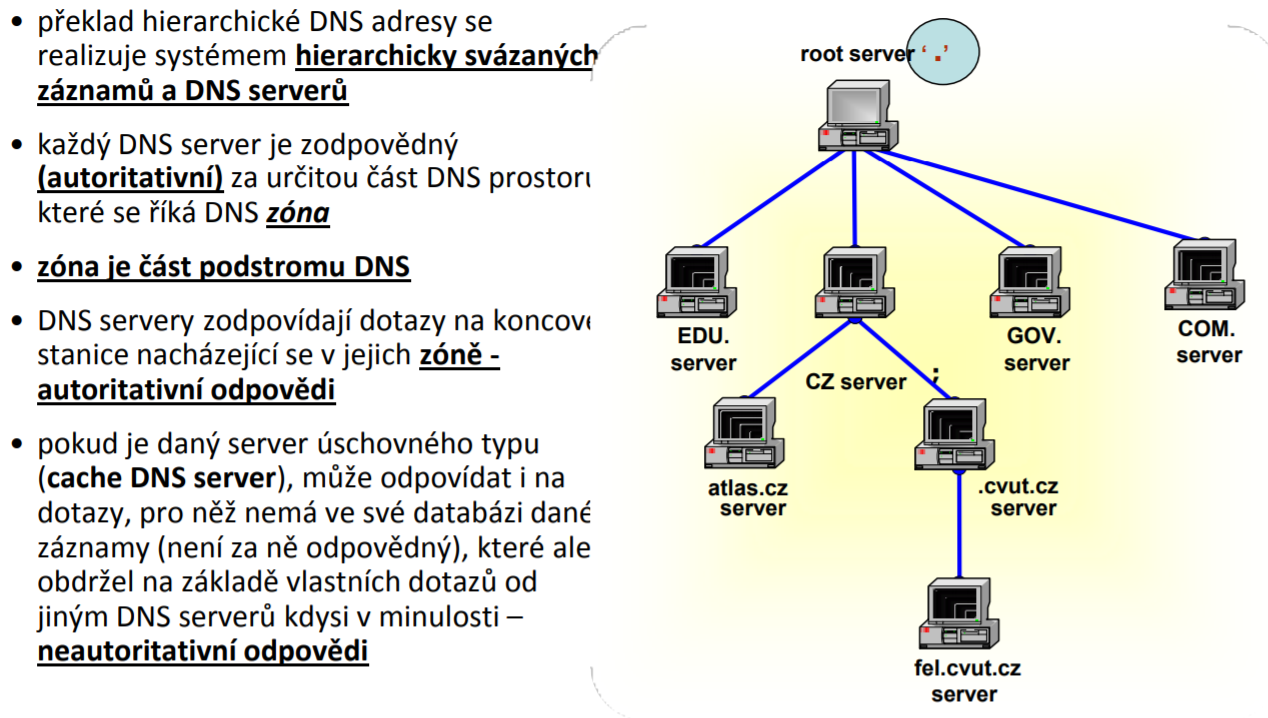
* systém jmen na němž je DNS založen tvoří hierarchickou stromovou strukturu, které se říká doménový jmenný prostor (domain name space)
* organizace (obecně subjekt) obdrží oprávnění k určité části jmenného prostoru, kam může přidávat další úrovně nebo koncové uzly
* DNS jména lze vytvářet bez přímé vazby na topologii IP sítě (výhoda); topologie sítě a DNS struktura jsou obecně na sobě nezávislé!!!!
* Systém DNS umožňuje efektivně udržovat decentralizované databáze doménových jmen a jejich překlad na IP adresy.



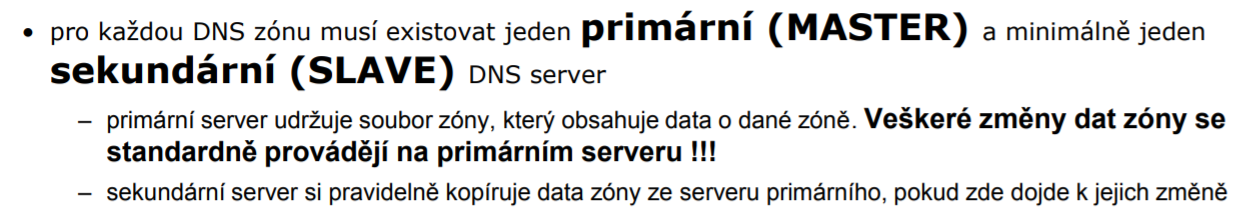
* Typy domén nejvyšší úrovně.



* Hierarchie DNS serverů. Co je autoritativní DNS server. Co je zóna DNS a jak se liší od DNS domény. Co je neautoritativní DNS (cache DNS).



* Primární a sekundární DNS servery. Kmenové DNS root servery.

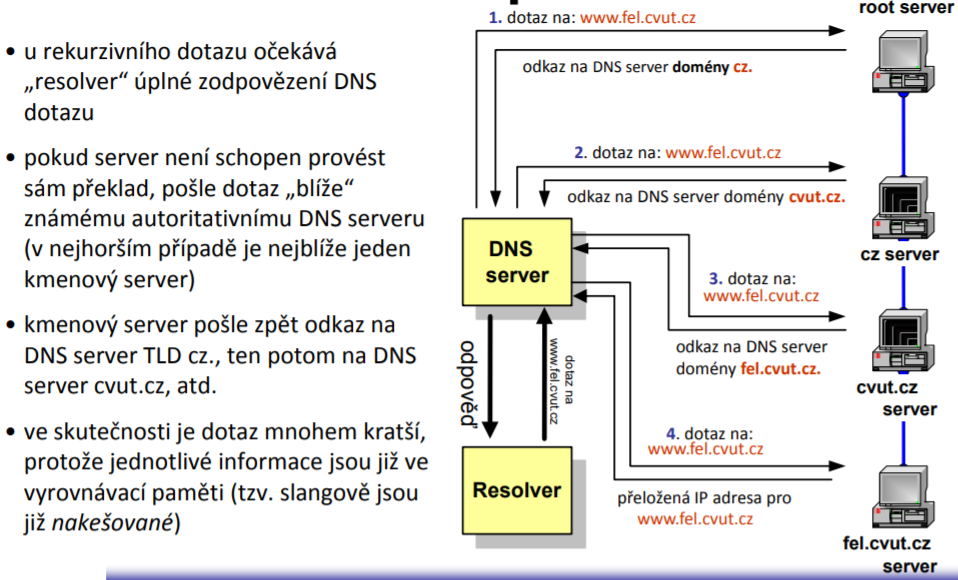


**DNS resolver**

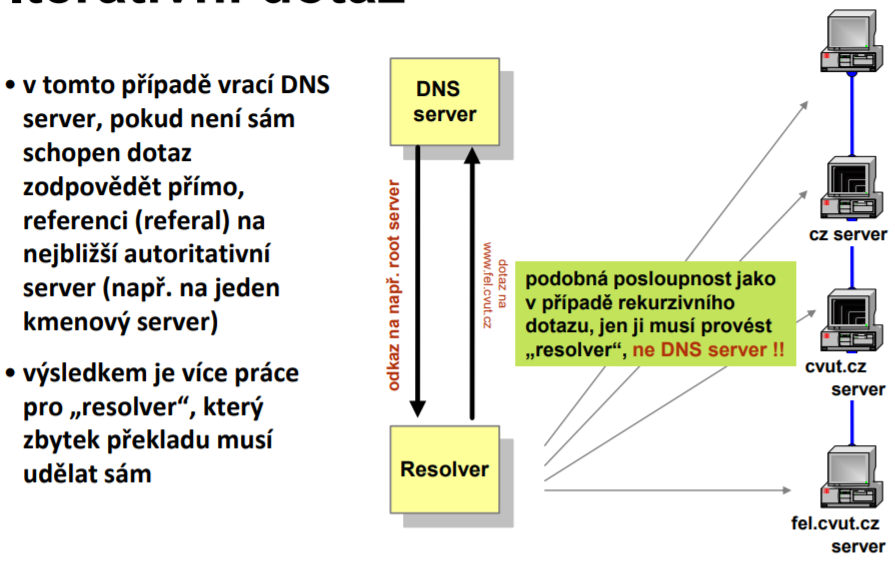
* A DNS resolver is a local server that stores a central database of DNS nameservers and manages DNS requests for all the clients on your network. With DNS resolvers, your computer does not need to store addresses for multiple online nameservers, a process which is difficult to manage effectively.
* DNS resolvers increase the efficiency of a DNS system. Without resolvers, every computer on a network would need to be provided with the addresses of several authoritative nameservers in order to resolve addresses.

**DNS server**

* The Domain Name System is maintained by a distributed database system, which uses the client–server model. The nodes of this database are the name servers.
* Popis funkce rekurzivního DNS dotazu.



* Popis funkce iterativního DNS dotazu.



## DHCP

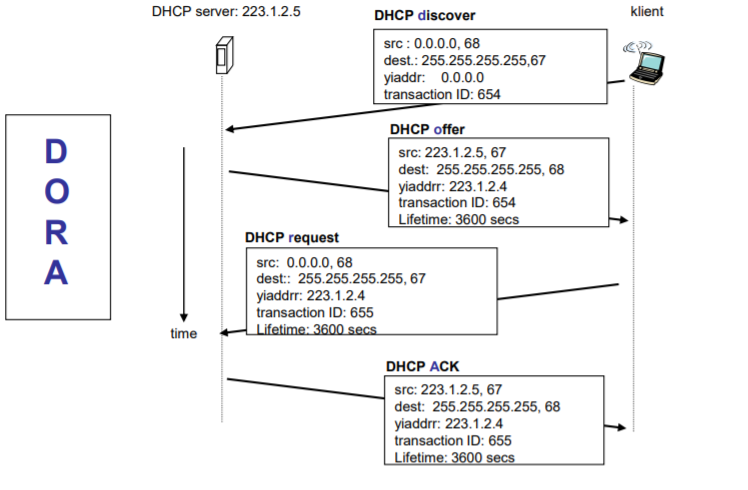
DHCP protokol umožňuje prostřednictvím DHCP serveru nastavovat stanicím v počítačové síti sadu parametrů nutných pro komunikaci pomocí IP protokolu.

Používá se pro automatickou konfiguraci počítačů připojených do počítačové sítě. DHCP server přiděluje počítačům pomocí DHCP protokolu zejména IP adresu, masku sítě, implicitní bránu (default gateway) a adresu DNS serveru.

Platnost přidělených údajů je omezená, proto je na počítači spuštěn DHCP klient, který jejich platnost prodlužuje.

Významným způsobem tak zjednodušuje a centralizuje správu počítačové sítě (například při přidávání nových stanic, hromadné změně parametrů nebo pro skrytí technických detailů před uživateli).

### Získání IP adresy



## NAT – Network Adress Translation

NAT odstiňuje konkrétní síť od zbytku globální sítě, tak, že zařízení uvnitř dokážou komunikovat směrem ven, ale externí zařízení se nedokážou přímo spojit se zařízeními v interní síti.

### Veřejné a privátní IP

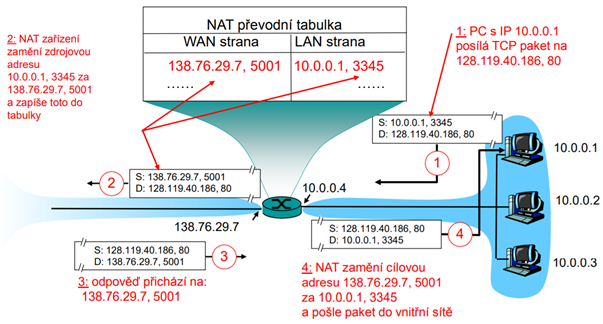
Privátní síť je v informatice označení pro počítačovou síť, která využívá speciální privátní IP adresy.

Privátní adresy jsou běžně používány pro domácí, kancelářské a podnikové lokální sítě (LAN), kde veřejné adresy (tj. globálně směrovatelné v internetu) nejsou žádoucí nebo nejsou dostupné.

### IP transformace

K zvýšení adresního prostoru se používá natting. Část počítačů je neveřejná pro internet, nemůže přímo komunikovat s internetem. Komunikují pouze přes jednu veřejnou IP adresu. K ní příslušný router si zaznamenává požadavky a zprostředkovává komunikaci mezi privátní a veřejnou sítí.

* NAT – pouze překlad adres
* PAT – k adresám se přiřazuje i port -> je možné mít v privátní síti duplikace adres



# Zabezpečení

## Ethernet – Filtrování MAC adres

Filtrace MAC adres umí nastavit to, že k vaší WiFi (k routeru) se mohou připojovat pouze zařízení, jejichž MAC adresu váš router zná.

Problém je, jak už bylo řečeno výše, že MAC adresu je možné síťovému rozhraní ručně nastavit – kdokoliv tak může dát svému zařízení MAC adresu zařízení jiného. Druhý problém je, že v každé sítí (WiFi i klasické) se MAC adresy objevují u všech paketů, které po sítí pobíhají.

## WPA – Zabezpečení bezdrátových sítí

WPA2 (Wi-Fi Protected Access 2) je dnes alespoň podle statistik projektu Wifileaks nejrozšířenějším způsobem zabezpečení Wi-Fi sítí v České republice. Existuje ve dvou variantách, WPA2-Personal (neboli WPA2-PSK), kde všichni klienti využívají stejné sdílené heslo a WPA2-Enterprise, který je po bezpečnostní stránce lepší, avšak díky nutnosti RADIUS serveru a složitější implementaci je vhodný, jak již z názvu plyne, spíše do podnikové sféry.

## HTTPS – Zabezpečení provozu

* HTTPS využívá protokol HTTP spolu s TLS. HTTPS je využíván především pro komunikaci webového prohlížeče s webovým serverem. Zajišťuje autentizaci, důvěrnost přenášených dat a jejich integritu.
* Bezpečnost komunikace zaručuje protokol SSL anebo novější TLS. Pomocí asymetrické kryptografie je ověřena identita webového serveru, volitelně i klienta.
* Poté následuje dohoda na klíči pro symetrické šifrování samotné komunikace (z výkonnostních důvodů). Klíč pro symetrickou šifru je buď vybrán klientem nebo dohodnut pomocí Diffieho-Hellmanovy výměny klíče pro dosažení dopředné bezpečnosti.
* TLS je zásadní infrastruktura veřejného klíče a X.509 certifikáty, díky nimž probíhá autentizace.
* Pro úspěšné ověření identity je nutná důvěra v zaslaný certifikát, která nejčastěji bývá zprostředkovaná některou z certifikačních autorit, jejichž certifikáty jsou v úložišti důvěryhodných certifikátů operačního systému nebo aplikace

# Další technologie

## Elektronická pošta

* **SMTP**: internetový protokol určený pro přenos zpráv elektronické pošty (e-mailů) mezi přepravci elektronické pošty (MTA). Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem; zpráva je doručena do tzv. poštovní schránky adresáta, ke které potom může uživatel kdykoli přistupovat (vybírat zprávy) pomocí protokolů POP3 nebo IMAP. Funguje nad protokolem TCP
* **IMAP**: (Internet Message Access Protocol) je internetový protokol pro vzdálený přístup k e-mailové schránce prostřednictvím e-mailového klienta. IMAP nabízí oproti jednodušší alternativě POP3 pokročilé možnosti vzdálené správy (práce se složkami a přesouvání zpráv mezi nimi, prohledávání na straně serveru a podobně) a práci v tzv. on-line i off-line režimu.
* **POP3**: je internetový protokol, který se používá pro stahování e-mailových zpráv ze vzdáleného serveru na klienta. Jedná se o aplikační protokol pracující přes TCP/IP připojení. Ze vzdáleného serveru se stáhnou všechny zprávy, třeba i ty, které uživatel číst nechce, nebo spam (pokud ho již nefiltruje poštovní server).