Internet

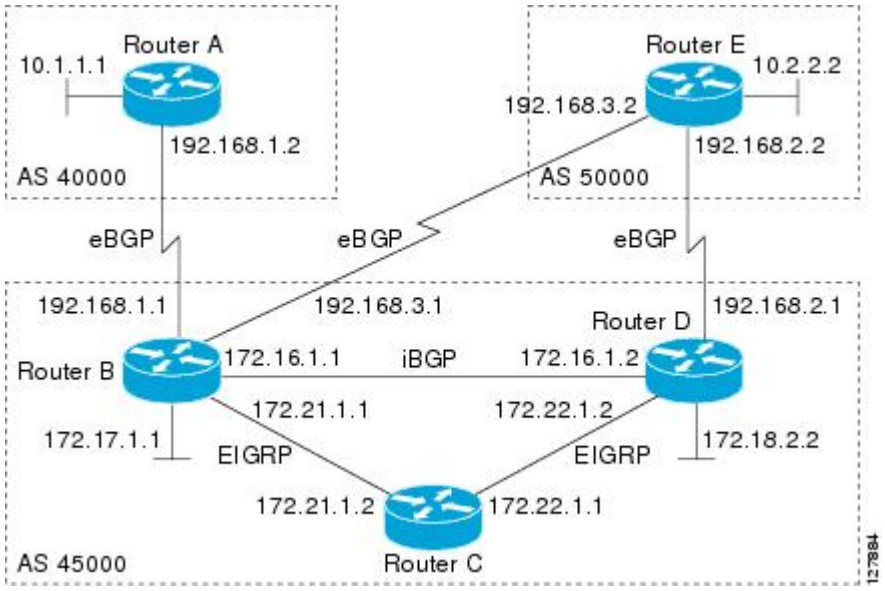
- net(work) – nějaká síť

- internet
  - propojení několika sítí
  - píše se s malým i

- Internet
  - ten Internet
  - technicky je to také propojení několika sítí
    - říká se jim autonomní oblasti
    - propojení je založeno na protokolu IP
      - internet může propojovat na základě jakéhokoliv protokolu, ale Internet je na základě IP – Internet Protocol
  - píše se s velkým I

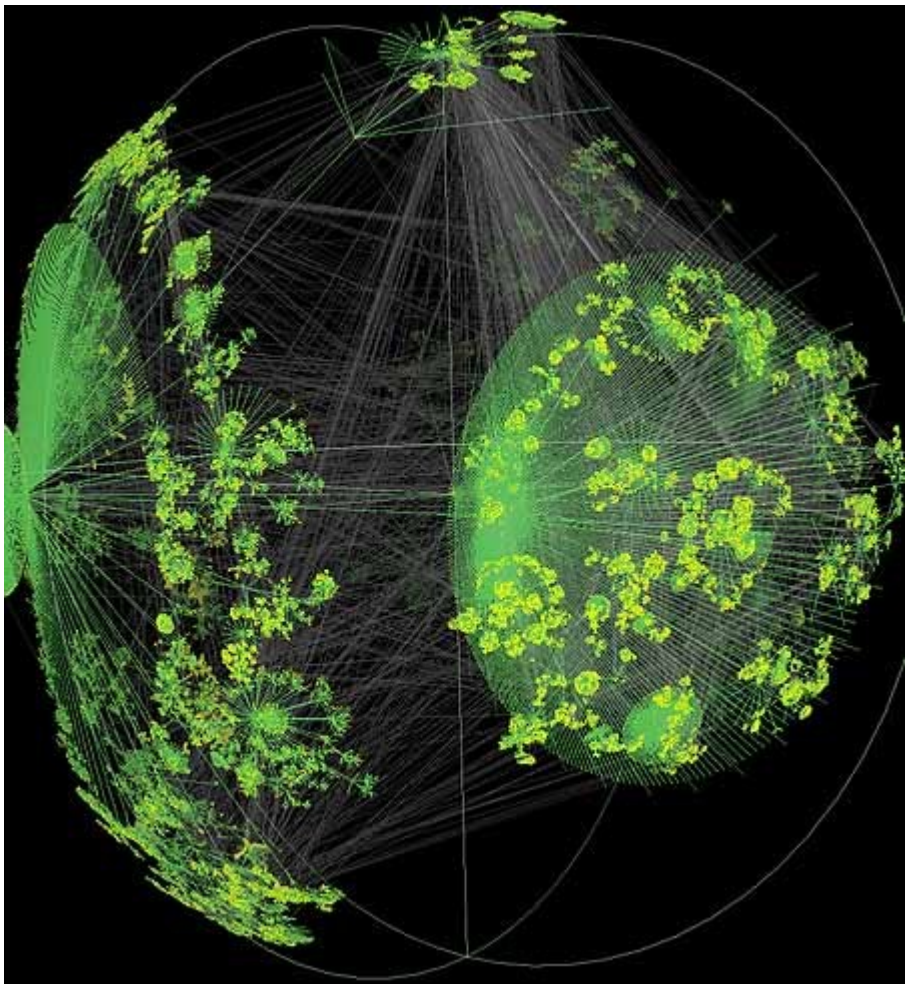
- intranet
  - soukromá část Internetu
  - například vnitřní síť firmy
  - interní informační portál ministerstva
  - intraweb
    - část intranetu, ve které jsou z protokolů vyšších vrstev pracovníky používány pouze protokoly HTTP a HTTPS
    - jinak lze používat i další protokoly, např. FTP

- extranet
  - intranet je omezen pro pracovníky organizace
  - extranet je přístupný pro další strany
    - zákazníci, dodavatelé, daňoví poplatníci…



http://www.cisco.com/en/US/docs/ios/12_4t/ip_route/configuration/guide/brbpeer.html

- Topologie Internetu



Source: Courtesy of Young Hyun, CAIDA

- Historie Internetu
  - V říjnu 1997 SSSR vypustil Sputnik a tím USA přišly o cenné body v žebříčku technologického závodu
  - Roku 1958 USA založily Advanced Research Project Agency, která měla ztracené body dohnat a SSSR zcela jasně předehnat
  - Součástí ARPA byla IPTO – Information Processing Technology Office
    - Vytvořili síť radarových stanic
  - Radarové stanice bylo třeba vzájemně propojit
    - V té době se používalo přepínání okruhů (circuit switching)
      - Taková síť není příliš robustní a v případě vyřazení klíčových bodů je prakticky k ničemu
        - Např. jaderný útok SSSR
    - Nové řešení se jmenovalo přepínání paketů (packet switching)
      - Robustní a flexibilní síť
      - Existuje v ní několik možných cest, takže je možné data doručit i po vyřazení většího části uzlů
        - Dokud se nepovede udělat řez grafem
  - V říjnu 1969 byly pomocí paketů propojeny dva uzly a vznikla tak síť ARPANet
    - Univerzitní prostředí
  - 1972 se ARPA přejmenovala na Defense ARPA, 1993 zpět na ARPA a 1996 opět na DARPA

- 1973 vzniká protokol NCP – Network Control Program
  - Předchůdce dnešního TCP/IP
- 1975 jsou propojeny dva počítače s protokolem TCP/IP
  - Univerzitní prostředí

- 1978 se spojila ARPANet s dalšími sítěmi z Evropy a Kanady
  - British Post Office, Telenet, DATAPAC, TRANSPAC
  - ARPANet je tak nejstarší ze sítí Internetu, který vzniknul jejich spojením
    - A postupným připojováním dalších sítí

- 1983 z ARPANet se vyčlenila část označená jako MilNet – Military Network
  - Síť pro výhradní použití DoD
  - Později označená jako Defense Data Network
  - Ještě později vznikly
    - NIPRNet
      - Unclassified but Sensitive Internet Protocol Router Network původně
      - Non-Classified Internet Protocol Router Network
      - Neutajovaná část vojenské komunikace

    - SIPRNet
      - Secret Internet Protocol Router Network
      - Utajovaná vojenská komunikace
        - Kompletně zabezpečený systém

- JWICS
  - Joint Worldwide Intelligence Communications System
  - Přenos Top Secret informací mezi DoD a DoState

- 1985 DARPA přijala TCP/IP jako standard pro vojenské účely

- 1985-6 National Science Foundation Network
  - Páteřní síť, propojení 6 superpočítačových center
  - 1,5 Mb/s, 10 000 počítačů

- 1988 Internet je otevřen pro komerční využití
  - Vznikli první komerční poskytovatelé připojení k Internetu – ISP (Internet Service Provider)

- 1987-1990 propojování regionálních sítí
  - 100 000 počítačů
- 1990-2 – NFSNet běží na 45 Mb/s
- 1994 – rozpad NFSNet na několik páteřních sítí
  - Internet se stává skutečně decentralizovaným

- 31. března 2008, 1,407 miliardy lidí používá Internet podle statistik Internet World Stats

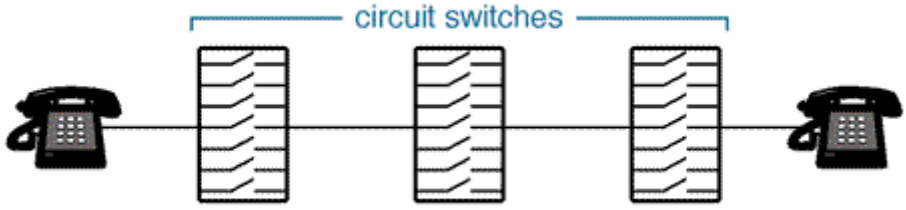
- Historie z pohledu nabízených služeb
  - 70. léta
    - sdílení výpočetních zdrojů
      - telnet
  - 80. léta
    - vzdálený přístup k souborům
      - File Transfer Protocol, Network File System, Andrew File System
    - E-mail
    - USENET – distribuovaný diskuzní systém
  - 90. léta
    - On-lince chat, instant messaging
    - Audio-video
      - Alternativa tradiční telefonní sítě
      - Alternativa tradičního rádia, CD, TV, …
    - www – alternativa tradičních novin a časopisů
  - A dále
    - Internetové bankovnictví
    - Peer 2 Peer sítě
      - I2P
    - Dopravní (silniční, letecké, …) informace
    - STAG ;-)
    - Virtuální život
      - Komunitní weby, seznamky, MMPORG, možnost publikovat pod pseudonymem
    - Na jednu stranu možnost sdělit svůj názor světu
      - Když vám to nikdo nezcenzuruje
    - Ale také možnost ztratit kontakt s reálným světem
    - A v neposlední řadě větší prostor a více příležitostí pro „ty špatný“
      - Zloději, hackeři a jiné existence

Přepínání okruhů

- Komunikují spolu pouze dva koncové uzly komunikační sítě
- Ty mezi sebou vytvoří tzv. komunikační okruh
  - Data lze posílat oběma směry
- Dokud spolu komunikují, nemohou komunikovat s nikým jiným

- První telefonní sítě
  - Spojovatelka manuálně spojovala příslušné vodiče – okruhy

  - První byla uvedena do provozu roku 1878 v Connecticutu
  - V roce 1891 pojal Almon Strowger, povoláním hrobník, podezření, že spojovatelka záměrně přepojuje hovory k jeho konkurenci
  - A tak vymyslel automatický volič, který počítal impulsy vyslané z telefonu volajícího a podle nich přepojoval
    - Počet impulsů odpovídal vytáčeným číslům



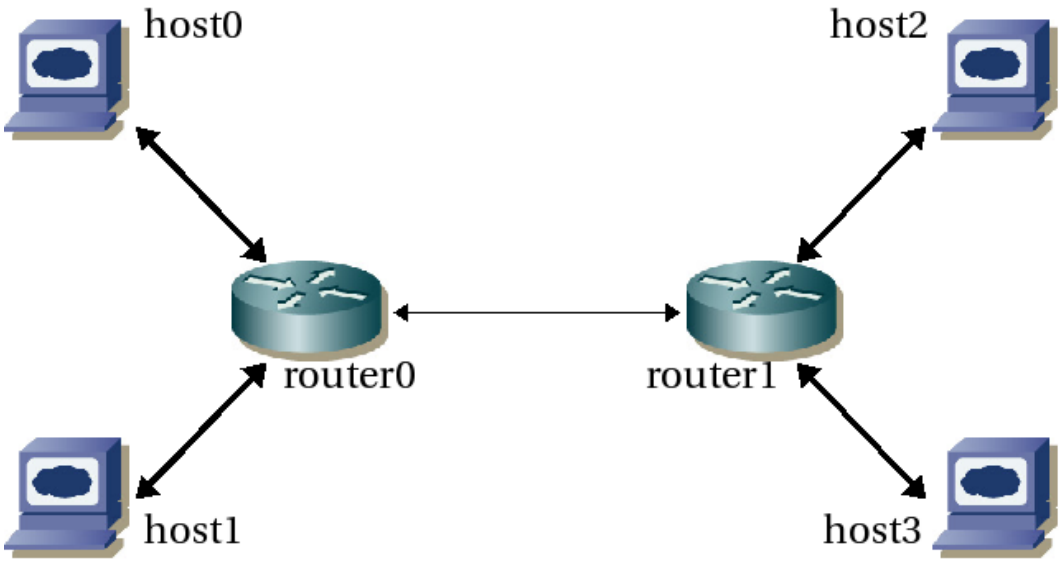
http://antibodynet.com/ascend/net_19.htm

- Postupem času se přešlo na přepínání paketů a okruhy se emulují – virtuální komunikační okruh
  - Např. pokud dnes voláte z mobilu

Přepínání paketů

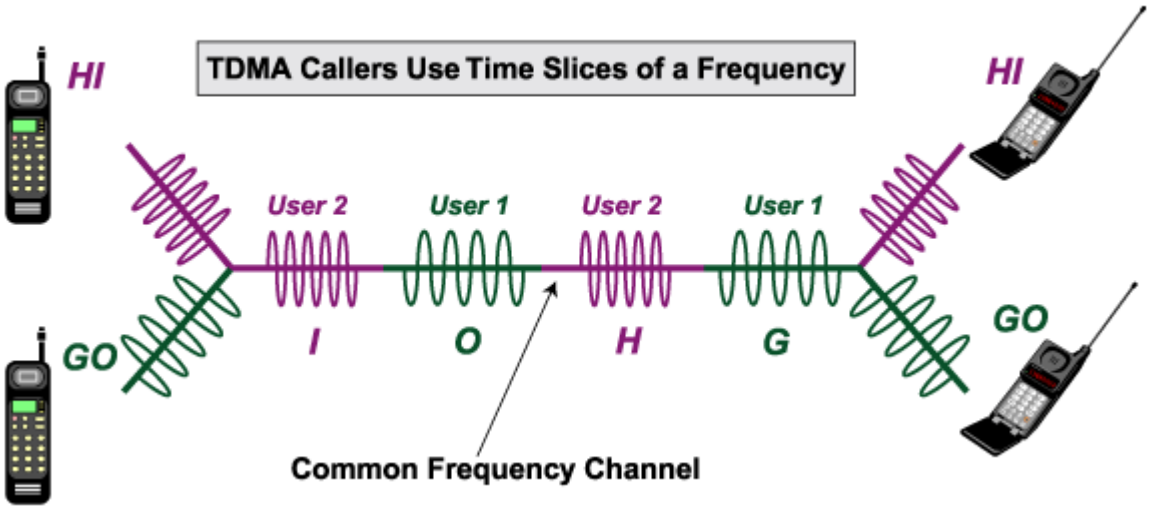
- Telefonní hovor je v podstatě proud po sobě jdoucích slov
- Paket by v takovém pojetí byla posloupnost po několika sobě jdoucích slov

- Okruhem se přenáší souvislý proud dat
- Proud dat se rozdělí na menší části a jednotlivé části se přenáší v paketech



http://ctieware.eng.monash.edu.au/twiki/bin/view/Simulation/ANetworkOf4HostsAnd2PacketSwitches

- Máme-li fyzicky k dispozici jenom jednu linku, která by kapacitně zvládla přenést dva hovory, pak
  - S přepínáním okruhů bychom mohli přenést pouze jeden hovor
  - S přepínáním paketů můžeme přenášet oba hovory současně
    - Voice over IP



http://www.pangolinsms.com/tech03-types-of-mobile-phones.htm

Duplex

- Režim komunikace mezi dvěma uzly
- Simplex
  - Data mohou jít pouze z jednoho uzlu do druhého
    - Tj. pouze jedním směrem
- Half Duplex
  - Data mohou jít oběma směry, ale ne současně
- Full Duplex
  - Data mohou jít oběma směry současně

Ethernet

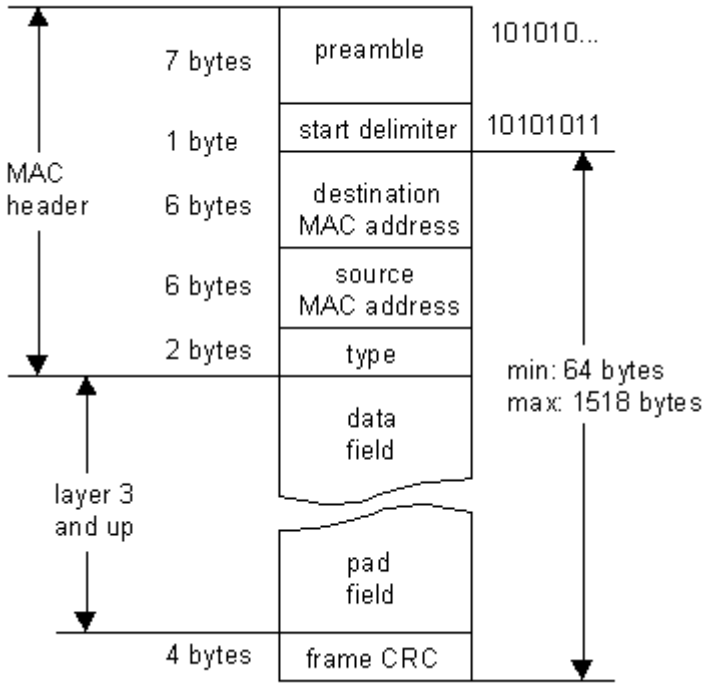
- Propojuje komunikační uzly

- Standard vícebodového sdílení komunikačního média
- Např. kabely UTP a STP
- Různé varianty
  - 10 Mb/s – koaxiální kabel, Ethernet
  - 10 Mb/s – UTP, Ethernet
  - 100 Mb/s – STP, Fast Ethernet
  - 1 Gb/s – Gigabit Ethernet
  - 10 Gb/s – 10 Gigabit Ethernet
    - Poslední varianty používají k přenosu buď optické vlákno, nebo kroucený měděný pár (do 100 m)
  - Varianty se liší rychlostí a maximální možnou délkou vedení
    - Existuje i minimální potřebná délka vedení
      - Dáno velikostí dat a rychlostí šíření signálu

- Ethernet stojí v hierarchii síťových protokolů úplně vespod
- Existují i jiné protokoly pro stejné užití
  - ATM, Sériový kabel, ..
    - K propojení uzlů lze použít i jiné prostředky, které k tomu nebyly přímo určeny
      - Paralelní kabel, FireWire, …

- Každý prvek připojený ke komunikačnímu médiu podle standardu Ethernet má tzv. fyzickou adresu – MAC
  - Media Access Control Address
  - Kóduje výrobce zařízení a sériové číslo zařízení
    - => má být jedinečná pro každé zařízení
  - Má 6 bytů

- Datové zprávy se přenášejí v tzv. rámcích
  - Další protokoly posílají pakety, které jsou zapouzdřeny právě v těchto rámcích
- Rámec má nějakou minimální a maximální velikost
- Rámec má hlavičku s adresami a dalšími užitečnými informacemi a prostor pro posílaná data
  - Posílaná data = paket



http://www.mattjustice.com/ethernet/layer2.html

Analogie vztahu Ethernetu a IP protokolu

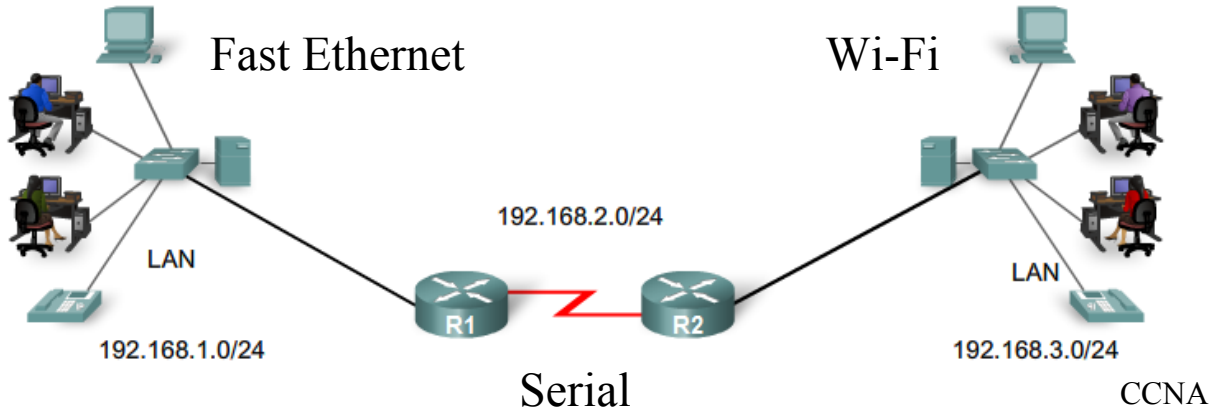
- Analogií k MAC může být číslo bytu v domě s výtahem bez schodiště (právě ho paní domácí umývá a nechce, aby jste tam hned šlapali;-)
    - Číslo bytu je jednoznačné právě jenom v konkrétním domě/vchodu panelového domu
        - Výtah je sdílené médium, které adresujete podle čísla bytu – nájemníci se jako reprezentace datových zpráv také musí nějak dohodnout, kdo zrovna pojede výtahem
            - Mají na to nějaký protokol k přístupu k výtahu – analogie Ethernetu
    - Pokud bychom chtěli adresovat jiný byt, nemůže k tomu použít pouze jeho číslo, protože bychom nerozlišili dům
    - => přidáme k němu poštovní adresu, která přesně určí konkrétní dům/vchod
        - Poštovní adresa je analogie k IP adrese
        - IP adresa je strukturovaná a proto IP protokol umožňuje směrování, na rozdíl od Ethernetu
            - Ale IP vám nevyřeší používání výtahu v domě
                - => takže potřebujete oboje
- Ethernet umožňuje doručení zprávy do konkrétního bytu na konkrétní poštovní adrese
    - Každý dům může používat jinou variantu Ethernetu, nebo jeho alternativu
- IP umožňuje doručení zprávy na konkrétní poštovní adresu

IP

- Hlavní protokol Internetu
  - Používají se dvě verze
    - v4 – dominantní
    - v6 – nástupce
    - pokud nebude výslovně uvedeno jinak, text se vztahuje k IPv4
    - Lichá čísla jsou experimentální verze, sudá pro ostré nasazení

- Internet Protocol
  - Nespojovaný protokol – Best Effort Delivery
  - Pakety jsou doručovány, ale v případě ztráty paketu se protokol nesnaží o jeho opětovné odeslání
    - Ztráta se nedetekuje, pouze s v některých případech úmyslně provádí
      - Např. při zahlcení sítě se méně důležité pakety zahodí, aby bylo možné doručit ty důležitější

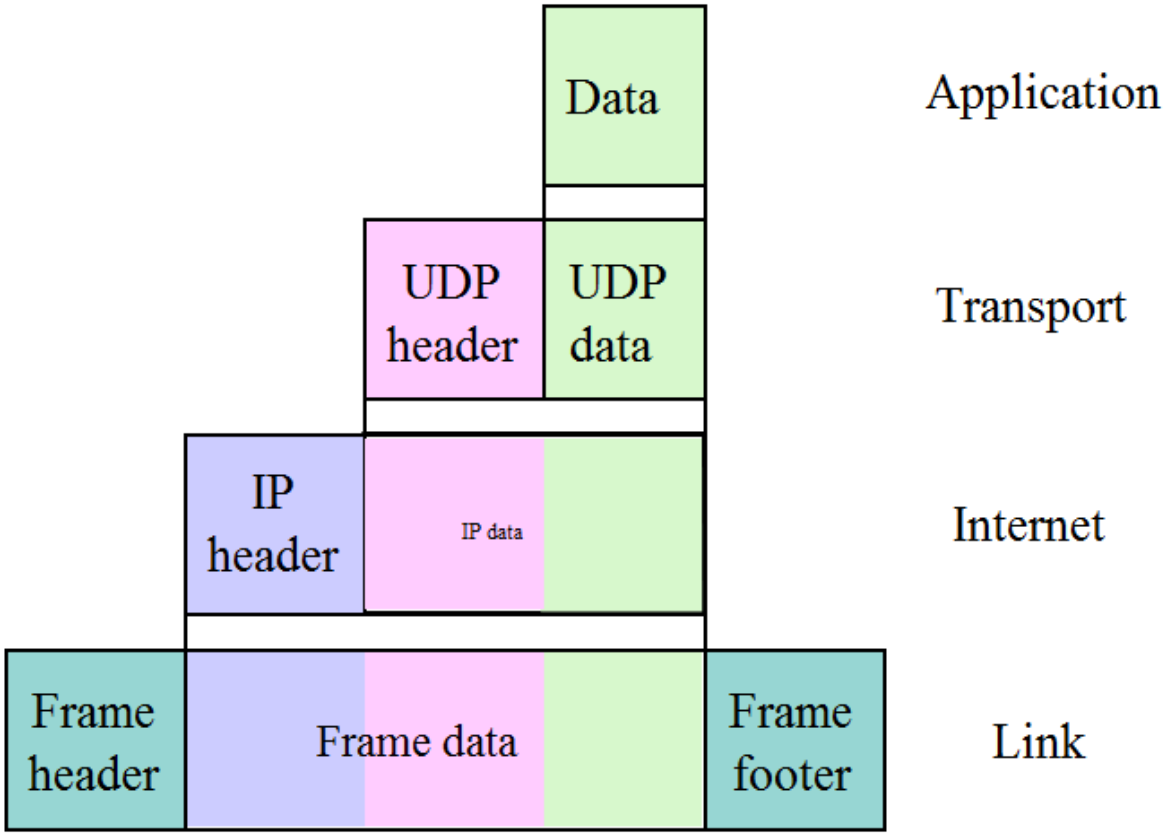
- Umožňuje vytvářet heterogenní síť, kde uzly jejích fragmentů spolu komunikují pomocí protokolů nižší úrovně
  - Ethernet, FDDI, ATM, Wi-Fi, …



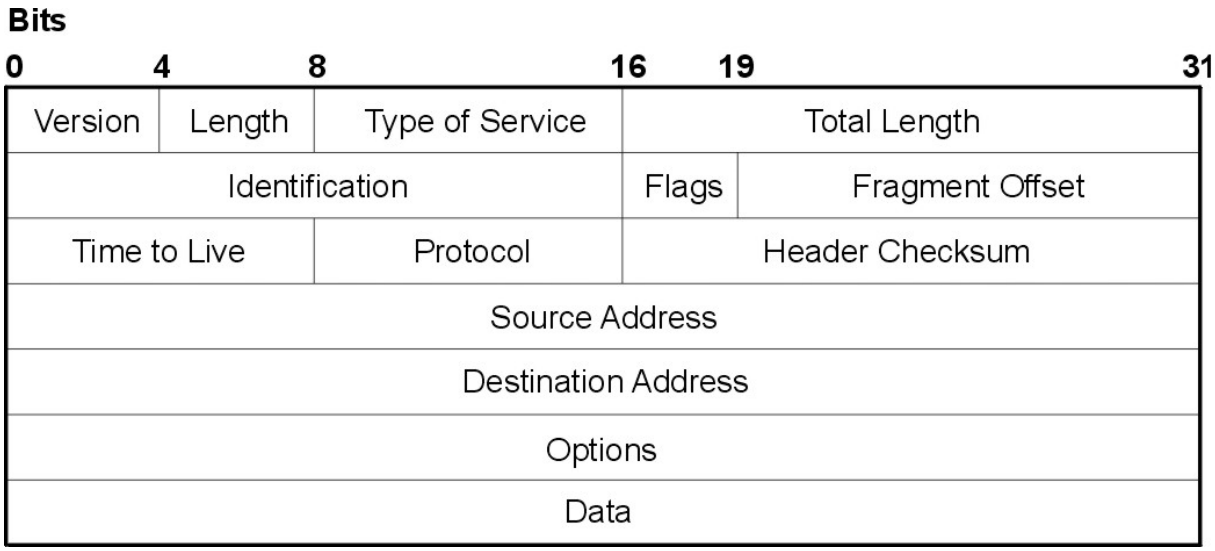
IP paket

- Datová zpráva protokolu
  - Obsahuj kdo, komu a co posílá
    - Plus další informace

- Nad protokolem IP jsou postaveny další protokoly, které přenášejí svá data uvnitř IP paketů
  - ICMP, UDP, TCP, …
    - A nad nimi jsou zase další protokoly
      - NTP, HTTP, …



http://en.wikipedia.org/wiki/Internet_Protocol



http://www.ncsa.uiuc.edu/UserInfo/Resources/Hardware/IBMp690/IBM/usr/share/man/info/en_US/a_doc_lib/aixbman/commadmn/tcp_protocols.htm

- Obrázek představuje IP paket
  - Data mohou mít pochopitelně větší velikost než 32 bitů
    - Jejich délka je proměnlivá a omezená maximální velikostí rámce, do kterého je paket zapouzdřen

- Důležité jsou všechny položky, ale pro rozsah KIV/ZPS vybereme jenom některé
  - Time to Live
    - Životnost paketu v síti – přirozené číslo
    - Paket se vytvoří s nějakou hodnotou větší než 0
    - Při každém průchodu uzlem se sníží o 1
    - Paket s TTL = 0 se zahodí
    - Cílem je, aby se nedoručitelný paket nepotuloval sítí do skonání světa
  - Protocol
    - Určuje protokol vyšší úrovně, jehož datová zpráva je uložena v datové části IP paketu
      - Např. UDP (17), TCP (6)

- Source Address
  - Adresa uzlu, ze kterého byl IP paket odeslán
- Destination Address
  - Adresu uzlu, do kterého má být IP paket doručen
- Data
  - Data posílaná v IP paketu

Protokoly a porty

- Aby počítač mohl pracovat s daným protokolem, musí být spuštěn program, který to umí
- Přijme-li počítač IP paket, podívá se na hodnotu položky Protocol a z ní určí, kterému programu předá paket k dalšímu zpracování
  - Pokud takový program nenajde, paket zahodí
- Některé tyto programy jsou součástí operačního systému

- Že počítač přijal IP paket zjistí např. tak, že se podívá do hlavičky přijatého ethernetového rámce a v položce Type najde hodnotu 0x0800 (2048 šestnáctkově)

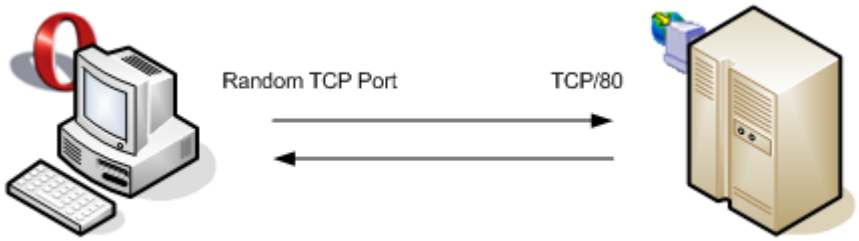
- Protokoly TCP a UDP, které používají protokol IP, zavádí ještě tzv. porty
  - Proto se píše TCP/IP a UDP/IP
- TCP i UDP využívá celá řada dalších protokolů (např. NTP, HTTP, FTP, Oscar (ICQ)), takže je nepraktické mít spuštěný jeden program pro TCP a druhý pro UDP
- Port je způsob, jak odlišit jednotlivé programy
  - Např. 21 pro FTP server a 80 pro HTTP server

- Analogie portu ke scénáři s domem
  - S IP se dostaneme na konkrétní poštovní adresu
  - S Ethernetem se dostaneme do konkrétních dveří
    - Např. kanceláře
  - S TCP/UDP portem se dostaneme ke konkrétnímu stolu, kde sedí hledaná osoba

- Máme spuštěný prohlížeč a chceme se podívat na dva různé www servery a vybrat poštu
  - Všechny použité protokoly používají protokol TCP
  - Vzdálené adresy, včetně portů
    - www.seznam.cz:80
    - www.zcu.cz:80
    - pop3.mail.cz:110
  - Na našem počítači, ze kterého k nim přistupujeme, nám operační systém pro každé připojení vygeneruje náš vlastní port – porty jsou na obou stranách

- Porty s číslem do 1024 jsou standardně rezervovány pro známé protokoly
  - Ve skutečnosti je jich víc
    - http://www.iana.org/assignments/port-numbers
  - Technicky však nic nebrání tomu, abychom na daném portu provozovali jiný protokol, než který je podle standardu očekáván
- Porty mimo vyhrazený rozsah jsou dostupné pro volné použití – např. pro navazování spojení se serverem

- Např. spojení s www.zcu.cz z HJ310
  - server (Apache): www.zcu.cz:80
  - klient (Opera): pc04-hj310.fek.zcu.cz:4103
    - port pro Operu dodá OS, Opera pracuje s HTTP a tak naváže spojení na portu 80



http://www.the-serpent.co.uk/net_works/www/http.php

IPv4 adresa

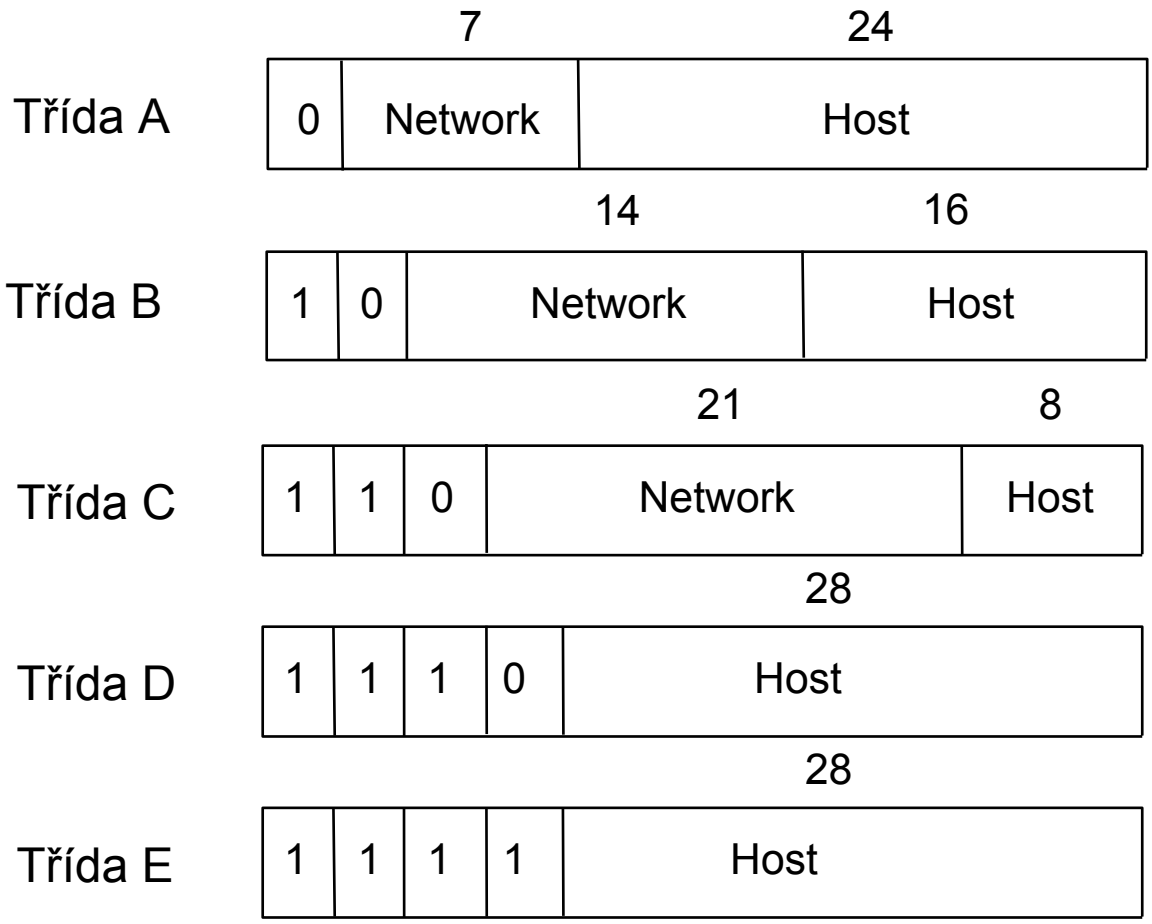
- skládá se ze čtyř bytů
  - zapisuje se po jednotlivých bytech v desítkové soustavě, oddělených tečkou
    - např. 147.228.42.20
  - tj. každé číslo je pouze v rozsahu 0 – 255

- je strukturovaná
  - skládá se z čísla sítě a z čísla počítače/uzlu
    - internet se skládá ze sítí a každá má své číslo
    - pokud se paket nenachází v cílové síti, je do ní nejprve doručen (směrování – viz později)
    - v cílové síti je doručen cílovému počítači

  - některé kombinace jsou vyhrazené a mají speciální význam
    - 127.0.0.1 – localhost – počítač, se kterým právě pracujete
    - 0.0.0.0 – neplatná adresa, nebo automatické zjištění IP adresy při konfiguraci sítě softwarem, případně aktuální síť (odesílající)
    - 255.255.255.255 – hromadná adresa, paket bude doručen všem počítačům v tzv. segmentu
    - A další…

- Historicky první rozdělení IP adresy
  - 1. byte číslo sítě
  - Zbývající 3 byty číslo počítače
  - To ovšem dávalo pouze 256 různých sítí, což bylo málo
    - Naopak 2^24 počítačů v jedné síti se ukázalo jako zbytečně příliš

- Proto došlo k zavedení adresních tříd



  - Každá IPv4 adresa začíná bitovým prefixem, ze kterého lze odvodit konkrétní třídu
  - Třídy A, B, C určují jeden konkrétní uzel
  - D je multicast
  - E je vyhrazeno pro budoucí užití

- Konkrétní třída určuje, které bity kódují číslo sítě a které číslo uzlu v konkrétní síti

- Multicast
  - Paket je doručen až několika uzlům
    - Tj. skupině příjemců
  - Doručení zajišťují speciální protokoly
  - Hodí se např. pro příjem videa

- Broadcast
  - Paket je doručen všem uzlům na dané síti
    - Všechny bity čísla uzlu v IPv4 adrese mají hodnotu 1
      - Např. 147.228.64.255
      - Např. 10.255.255.255
    - Speciální hodnota 255.255.255.255 označuje všechny počítače na tzv. segmentu sítě

- Postupem času došlo k vyčerpání adresního rozsahu, protože třídy A zabíraly zbytečně mnoho prostoru, aniž by byl využit – jak ho rozdělit?
- Řešením se stal nový způsob, jak vyjádřit, které bity určují číslo sítě
  - CIDR – Classless Inter-Domain Routing
    - Předchozí je classful
    - Založen na VLSM
  - VLSM – Variable-Length Subnet Masking

  - 147.228.64.0
    - Číslo sítě třídy C
    - Číslo uzlu má v takovém případě vždy všechny bity rovny 0 (konvence zápisu)

147.228.64.132/24

- Za lomítkem je počet bitů, které určují číslo sítě
- 132 – číslo za lomítkem = bity určující číslo uzlu v síti
- Číslo sítě je 147.228.64.0

- Síťová maska
  - 147.228.64.132 255.255.255.0
  - Provede se logická operace AND a ta nám určí číslo sítě

```
10010011 11100100 01000000 10000100
11111111 11111111 11111111 00000000
                    AND
10010011 11100100 01000000 00000000
```

  - Číslo sítě je 147.228.64.0

  - Např. manuální konfigurace síťového připojení ve Windows, ale nejenom tam, se provádí pomocí síťové masky
    - Poskytuje ISP;-)

- Aby mohl počítač v IP síti správně fungovat, musí mít k IP adrese přiřazenu správnou síťovou masku
  - Pokud má např. jinou síťovou adresu než směrovač, který směruje vaše pakety do Internetu, pak mohou být každý (váš počítač a směrovač) na jiné síti a vy se nemusíte dostat na Internet
    - Proč nelze napsat vždy souvisí s technikami supernetting a subnetting, které jsou ale mimo rozsah KIV/ZPS
      - Jde o slučování a dělení adresních rozsahů

- IPv4 adresa dává dohromady 2^32 adres mínus vyhrazené kombinace
- Kromě nich jsou však ještě vyhrazeny bloky v adresním prostoru, které mají speciální význam
- Pro rozsah KIV/ZPS nás zajímají tzv. privátní adresy

Privátní IPv4 adresa

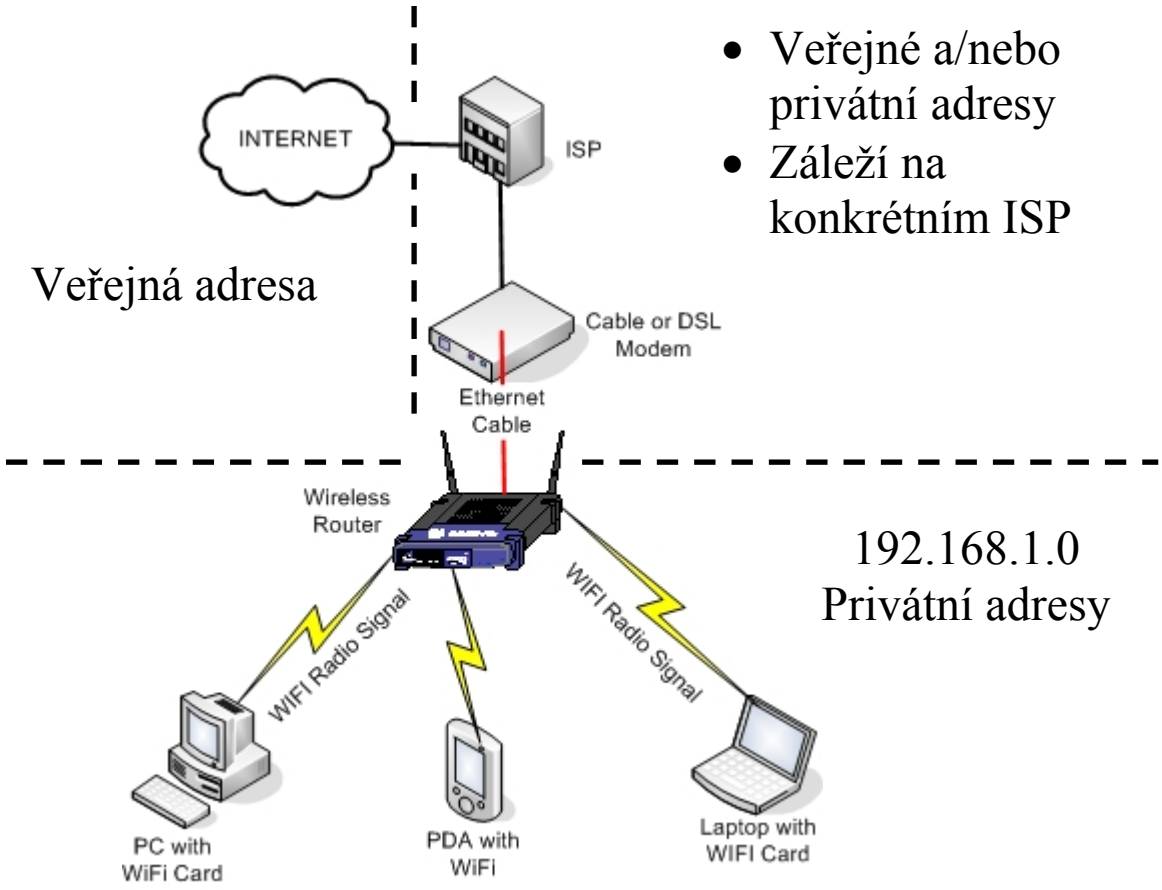
- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

- Řídí se těmi samými pravidly jako právě diskutované adresy – většinou veřejné
  - Existují totiž vyhrazené bloky adres, které jsou např. experimentální

- Privátní adresy nejsou směrované v Internetu
  - Tj. nemůže je mít žádný server, který má být celosvětově přístupný
  - Tyto adresy jsou směrované pouze v rámci sítě svého provozovatele

- Způsob, jak „nafouknout“ malý adresový prostor
  - Např. ISP přiděluje klientům pouze privátní adresy a navenek vystupuje pouze s jednou veřejnou adresou

- Obvyklé použití je např. domácí wi-fi síť, kdy je směrovač předkonfigurován přidělovat adresy v síti 192.168.1.0



- Veřejné a/nebo privátní adresy
- Záleží na konkrétním ISP

http://www.networkingreviews.com/2008/03/04/home-network-setup-wireless-home-network/

- Veřejné IP adresy jsou pronajímány
- Privátní IP adresy jsou zadarmo

- Protože nejsou v Internetu směrované, může si každý doma postavit svou vlastní síť
  - Např. váš notebook může mít 192.168.1.43 a počítač vašeho souseda u stejného ISP také

- Protože se privátní adresy v Internetu nesměrují, potřebujeme další mechanismus, která nám umožní komunikovat s veřejnými adresami – NAT

- Nelze navázat spojení mezi dvěma privátními adresami, jestliže cesta mezi nimi pro to není specificky nakonfigurovaná – v případě Internetu to není nikdy
  - => Internetový server musí mít veřejnou adresu

Spojované a nespojované protokoly

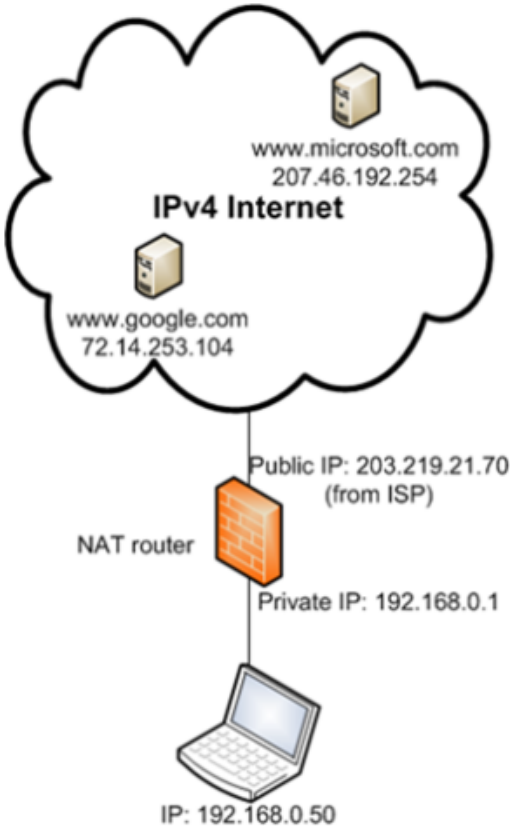
- Nespojované protokoly
  - Connectionless Protocols
  - Data jsou posílána v tzv. datagramech, které jsou zapouzdřeny v paketech
    - Datagram má maximální možnou velikost
  - Datagramy jsou odeslány, ale protokol se už nestará o doručení potvrzení, že byly skutečně doručeny
  - UDP
    - NTP, TFTP, DNS (po jednom požadavku)

- Spojované protokoly
  - Connection-Oriented Protocols
  - Data se posílají v tzv. proudech, jejichž velikost není omezena
  - Protokol zajišťuje, že jsou doručena všechna odeslaná data a to v odeslaném pořadí
    - Pokud se některý paket ztratí, je znovu odeslán
  - TCP
    - HTTP, FTP, DNS (více požadavků)

- Spojovaný protokol naváže spojení a dokud nedojde k chybě, nebo k jeho řízenému ukončení, tak je považováno za aktivní
  - Díky tomu si uzel sítě může zapamatovat, zda přes něj vede konkrétní spojení realizované spojovaném protokolem postaveným např. na TCP

NAT

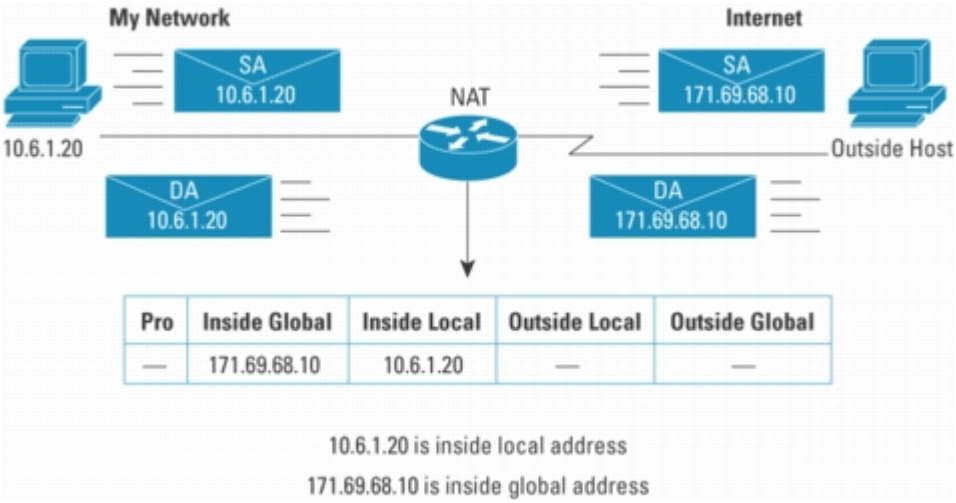
- Network Address Translation
- Jestliže mám privátní adresu, jak budu komunikovat se serverem s privátní adresou?



http://ozgrant.com/2007/09/16/teredo-tunneling-pseudo-interface-and-ipv6/

- Z privátní adresy lze poslat paket na veřejnou adresu
  - Příjemce však uvidí poslední (na cestě od něj) veřejnou adresu, ze které paket přišel a tu bude považovat za odesílatele
    - Tj. NAT router
- Pokud tedy uzel s veřejnou adresou odešle paket v odpovědi, paket se dostane na NAT router, protože nebyl adresován konkrétnímu počítači v privátní síti
  - Nespojovaný protokol tedy nelze použít
    - Pokud není nainstalován Port Address Translation – mimo rámec KIV/ZPS

- Naproti tomu spojovaný protokol udržuje spojení aktivní, tj. NAT router ví, který počítač v privátní síti komunikuje s uzlem s veřejnou adresou



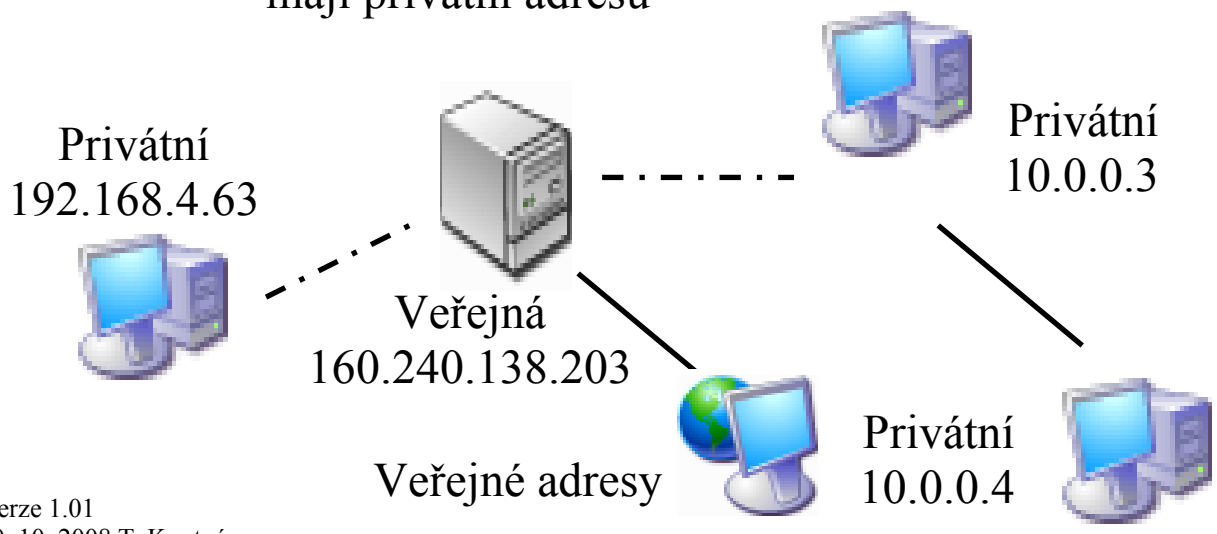
http://www.cisco.com/en/US/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9_ps6640_Products_White_Paper.html

- NAT router udržuje tzv. NAT tabulku, ve které je zapsáno, kdo s kým komunikuje
  - Řádek tabulky obsahuje dvojice adresa:port uzlu v privátní síti a uzlu, se kterým komunikuje
    - Včetně dalších, potřebných informací
      - Mimo rámec KIV/ZPS
  - Podle této tabulky se přepisují adresy IP paketů
    - NAT router do odchozího paketu napíše svou veřejnou adresu jako zdrojovou
    - Uzel mimo privátní síť na tuto adresu pošle odpověď
    - NAT přepíše cílovou adresu příchozího IP paketu adresou uzlu v privátní síti, se kterým je navázáno spojení

- Může se stát, že dva uzly v privátní síti budou chtít komunikovat s uzlem mimo privátní síť
  - Mimo rámec KIV/ZPS, pro zajímavost
  - Např. webový server, kdy oba použijí stejný cílový port – 80
  - Protože uzel mimo privátní síť vidí adresu NAT routeru, situace se může zkomplikovat ještě tím, že oba uzly v privátní sít použijí stejný zdrojový port
  - Bez dalších opatření, NAT router by tak nevěděl, kterému z daných dvou uzlů předat příchozí data
    - Jednou z možností je překládat i porty tak, aby z NAT routeru nikdy neodcházely dvě různá spojení se stejným zdrojovým portem
    - Anebo router prostě odmítne navázat spojení

- Chtějí-li spolu přes Internet komunikovat dva uzly, každý s privátní adresou, potřebují další uzel s veřejnou adresou, který jim bude jejich data přeposílat (čerchovaně

- Stále důsledek toho, že se privátní adresy v Internetu nesměrují
  - Toho využívají např. p2p sítě jako Direct Connect, nebo Donkey
    - Server hraje roli prostředníka, když oba klienti mají privátní adresu



IPv6

- Hlavní problém IPv4, který odstraňuje IPv6, je nedostatek veřejných adres
  - Většina Internetu ale stále ještě používá IPv4
- IPv6 adresa má 128 bitů
  - 665,570,793,348,866,943,898,599 adres na 1m^2
    - Povrch Země je 511,263,971,197,990 m^2
- IPv6 díky svému adresnímu rozsahu nemá privátní adresy
  - Odpadá tak maškaráda s NATem
    - Termín maškaráda se skutečně používá
  - A souboj Classful vs. CIDR & VLSM už nemá význam
- Změna adresy není jediná, ale je nejvíce patrná
  - Ostatní jsou mimo rámec KIV/ZPS

- Adresa se zapisuje po 4 číslicích v šestnáctkové soustavě (tj. 2 byte) oddělených dvojtečkou
  - Úvodní nuly lze vynechat
  - Posloupnost nul lze nahradit dvěmi dvojtečkami

  - `2001:0db8:0000:0000:0000:0000:1428:57ab`
  - `2001:0db8:0000:0000:0000::1428:57ab`
  - `2001:0db8:0:0:0:0:1428:57ab`
  - `2001:0db8:0:0::1428:57ab`
  - `2001:0db8::1428:57ab`
  - `2001:db8::1428:57ab`

  - ::1 je localhost

- Lze použít i CIDR zápis
  - `2001:0db8:1234::/48`
    - `2001:0db8:1234:0000:0000:0000:0000:0000`
    - `2001:0db8:1234:ffff:ffff:ffff:ffff:ffff`

DNS

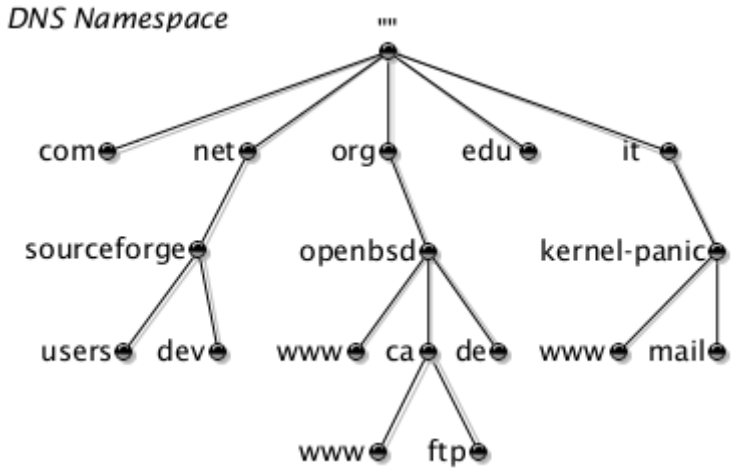
- Domain Name System
- Kdo by si pamatoval adresy svých oblíbených stránek jako sekvence 2^32, nebo dokonce 2^128, čísel?
- Cílem je umožnit adresovat počítače v lidsky čitelné podobě namísto sekvence čísel
    - Např. www.zcu.cz namísto 147.228.57.100

- Jméno uzlu se udává ve tvaru host.subdoména.doména, přičemž subdomén může být několik
    - Např. www.zcu.cz
        - cz je doména nejvyšší úrovně
            - TLD – Top Level Domain
        - zcu je doména druhé úrovně
            - SLD – Second Level Domain
        - www je název hostitele webového serveru
            - www není povinné, je to zvyklost

    - např. www.san.zcu.cz
        - san je doména třetí úrovně

- úroveň domény klesá zprava doleva

- absolutní jméno uzlu obsahuje výčet všech domén
    - FQDN – Fully Qualified Domain Name
        - Jméno hostitele a výčet všech domén
        - www.zcu.cz, korektně s tečkou www.zcu.cz**.**
- neúplné (relativní) jméno uzlu může obsahovat např. pouze jméno hostitele, který se nachází v aktuální doméně
    - např. www v doméně zcu.cz



http://www.kernel-panic.it/openbsd/dns/dns2.html

- TLD mají kořenovou doménu *root*
  - Označuje se pouze tečkou
    - Proto www.zcu.cz.

- původně byly doménová jména nejvyššího řádu pojmenovány podle typu obsahu
  - edu – education
  - com – company
  - net – networking (ISP)
  - gov – government
  - mil – military
  - org – organization (např. IEEE, ACM, houbaři.org)

- později byl jejich seznam rozšířen, např. o
  - biz
  - info
  - name

- mezitím byly rozšířeny o domény dle geografického rozdělení:
  - cz
  - cs – historická, pro Československo

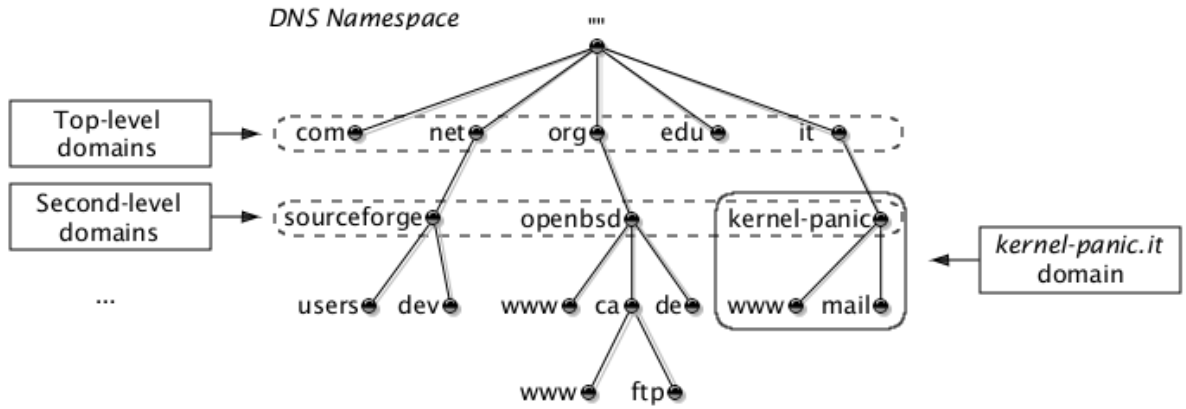
Protokol DNS

- Převádí IP adresy na doménové jména a zpět
- Jedna IP adresa může mít několik doménových jmen
  - Např. základní varianty webhostingu
- Jedno doménové jméno může mít několik IP adres
  - Např. zpravodajský web s tak velkou návštěvností, že by to jeden server nezvládnul

- Používá protokoly UDP a TCP

- DNS server
  - Může poskytuje i další informace o oblasti
    - Jmenné servery
    - Poštovní servery
    - Informace o doméně
    - Doba platnosti záznamu
    - PTR – viz převod IP adresy na FQDN
    - A další mimo rozsah KIV/ZPS

- V každé oblasti je jeden primární server
  - Zde se modifikují záznamy
- A jeden sekundární server
  - Který získává informace z primárního serveru
  - Zvýšení spolehlivosti
- DNS servery dohromady tvoří distribuovanou databázi



http://www.kernel-panic.it/openbsd/dns/dns2.html

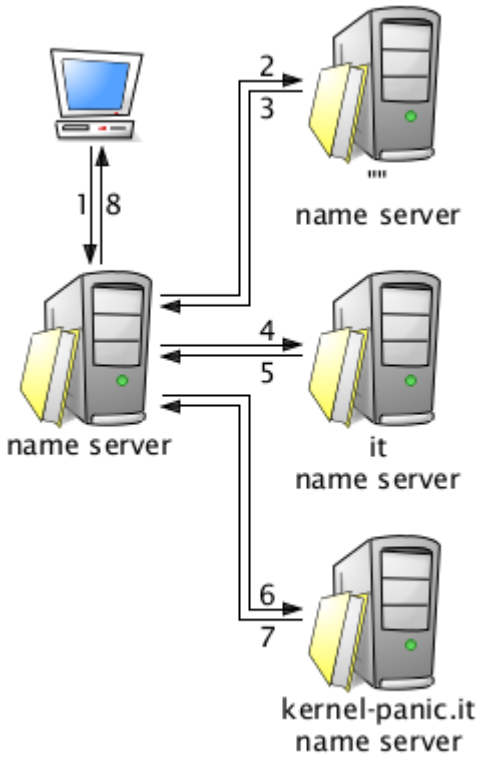
- Hierarchie domén může nějakým způsobem odrážet hierarchii organizace
  - www.kiv.zcu.cz
- Každá z domén má své DNS (jmenné) servery
  - Servery tvoří hierarchii

- GLTD
  - General Top Level Domain
  - 13 DSN *root* serverů
    - A.ROOT-SERVERS.NET
    - B.ROOT-SERVERS.NET
    - …
    - M.ROOT-SERVERS.NET

  - Poskytují informace o doménách druhé úrovně
    - DNS servery druhé úrovně poskytují informace o doménách třetí úrovně
      - Atd.

- Informace o serverech jsou zapsány pomocí doménových jmen, protože IP adresy se mohou změnit
  - Nicméně, na začátku potřebujeme alespoň IP adresu jednoho *root* serveru, abychom mohli převádět

- Převod doménového jména na IP adresu
  - Aneb, co se stane, když v prohlížeči zadáte adresu
  - Prohlížeč požádá operační systém o navázání spojení s *www.kernel-panic.it*
  - Operační systém se podívá do svých záznamů, zda je v nich IP adresa pro dané jméno
  - Pokud tam není, pak



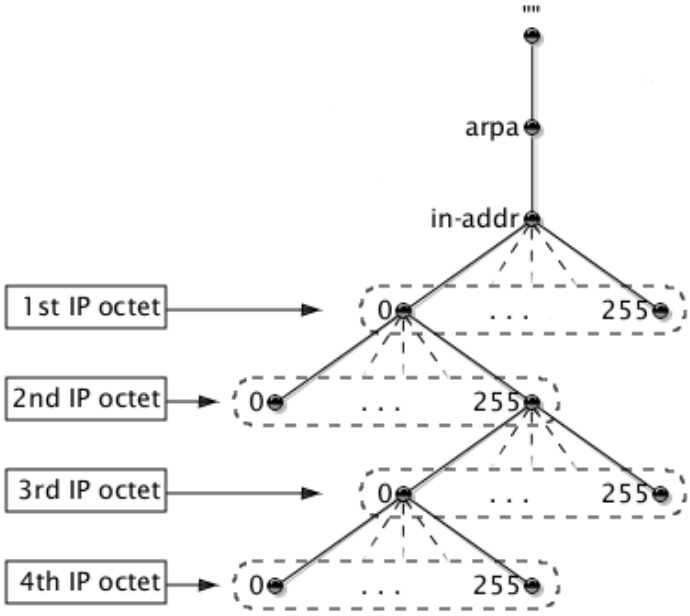
http://www.kernel-panic.it/openbsd/dns/dns2.html

1. pošle rekurzivní dotaz serveru ve své doméně
2. ten však nespravuje doménu .it a tak se zeptá kořenného serveru na adresu .it serveru
4. pak se zeptá .it serveru na cílovou doménu
6. a následně se zeptá jmenného serveru domény kernel-panic.it na cílovou adresu
8. jmenný server vrátí získanou IP adresu operačnímu systému vašeho počítače a ten s ní pak naváže spojení

- Jsou dva typy DNS dotazů
  - Rekurzivní – DNS server buď vrátí chybu, nebo úplnou odpověď
  - Iterační – DNS server vrátí nejlepší odpověď, kterou zná

  - Operační systém se zeptal rekurzivně DNS serveru ve své doméně, a ten se ptal iterativně ostatních DNS serverů

- Převod IP adresy na FQDN
  - Pro zajímavost, jinak mimo rozsah KIV/ZPS



http://www.kernel-panic.it/openbsd/dns/dns2.html

  - Speciální doména in-addr.arpa (pro zadání dotazu)
  - Reverzně zapsaná IP adresa www.zcu.cz (147.228..)
    - 100.57.228.147.in-addr.arpa
  - 4 úrovně vnoření uzlů, každý má 256 pod-uzlů
    - Odpovídají IP adrese
    - Pod-uzel má PTR záznam, který říká, který server zná další část stromu
      - => distribuovaná databáze
  - S listem (4. byte) dostaneme FQDN