Sítě a internet

Počítačová síť

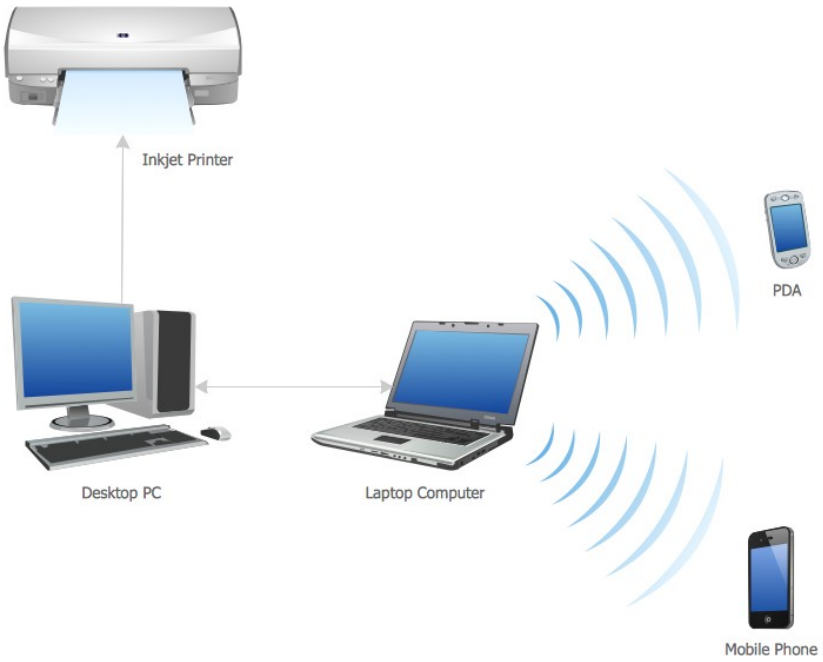
„Počítačová síť je vzájemné propojení dvou a více počítačů“

Počítačová síť

- Síť je založena na splnění 2 základních podmínek:
- 1) síťový hardware - umožňuje fyzické propojení počítačů:
  - kabeláž, síťová karta, aktivní síťové prvky (switche, routery…)
- 2) síťový software - postará se o vlastní přesuny dat od navázání spojení přes zabezpečení, kontrolu apod. Jedná se o ovladače, firmware, ovládací SW, aplikace apod.

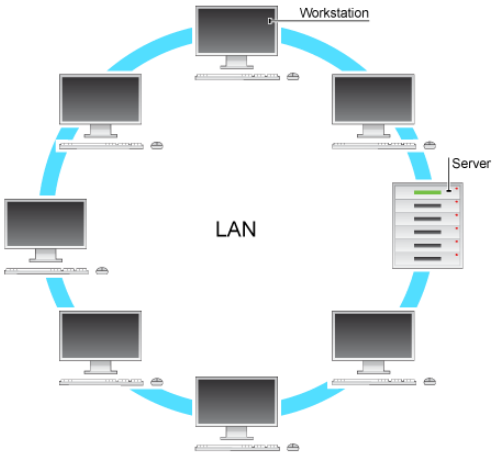
Dělení počítačových sítí

- PAN - Personal Area Network
  - Osobní síť
  - Velice malá, několik metrů okolo jednotlivce
  - Příklad: propojení mobilu s notebookem přes bluetooth



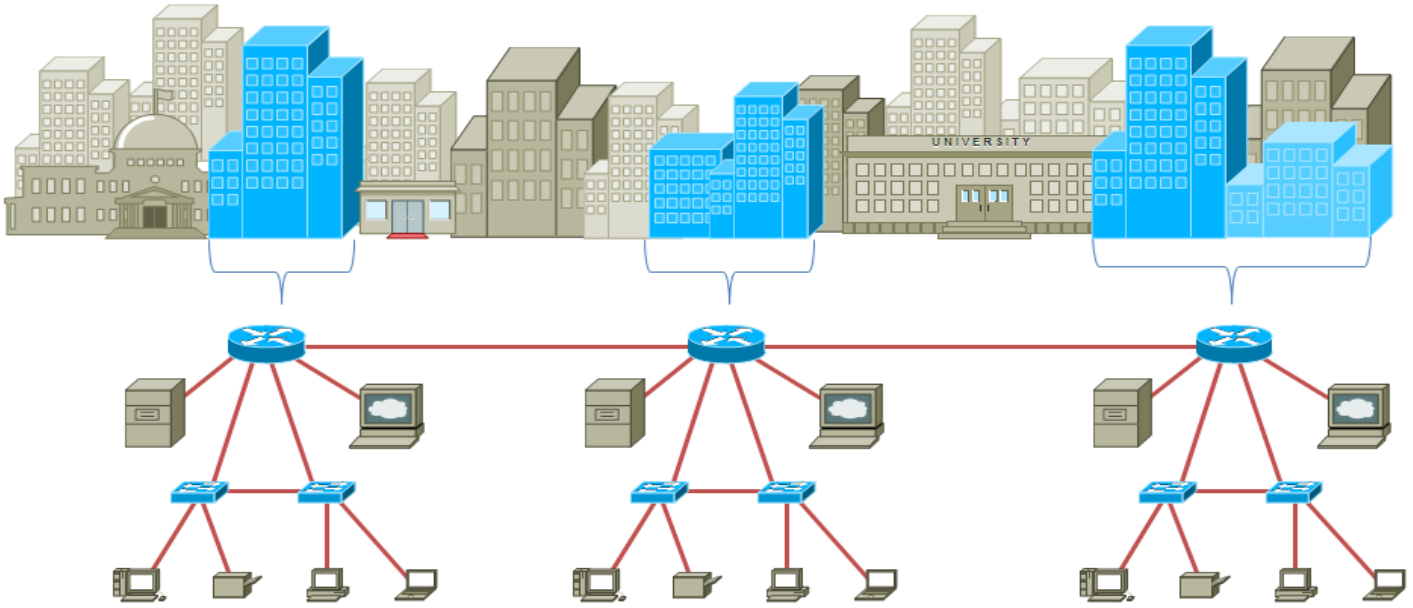
Dělení počítačových sítí

- LAN – Local Area Network
  - Menší síť propojující zařízení (PC, tiskárny…) v jedné domácnosti, budově, nebo několika přilehlých budovách.
  - Do několik stovek metrů maximálně, nejčastěji se však setkáváme s malými LAN sítěmi v domácnostech
  - Nejčastěji propojeny přes routery a switche



Dělení počítačových sítí

- MAN – Metropolitian Area Network
  - Velká síť na úrovni města
  - Síť propojující lokální sítě v městské zástavbě, spojuje vzdálenosti řádově jednotek až desítek kilometrů



Dělení počítačových sítí

- WAN – Wide Area Network
  - Velké sítě, spojujích mnoho LAN sítí do jednoho celku
  - Sítě zahrnující několik kontinentů, celosvětové sítě
  - Nejvýznačnější WAN síť - INTERNET

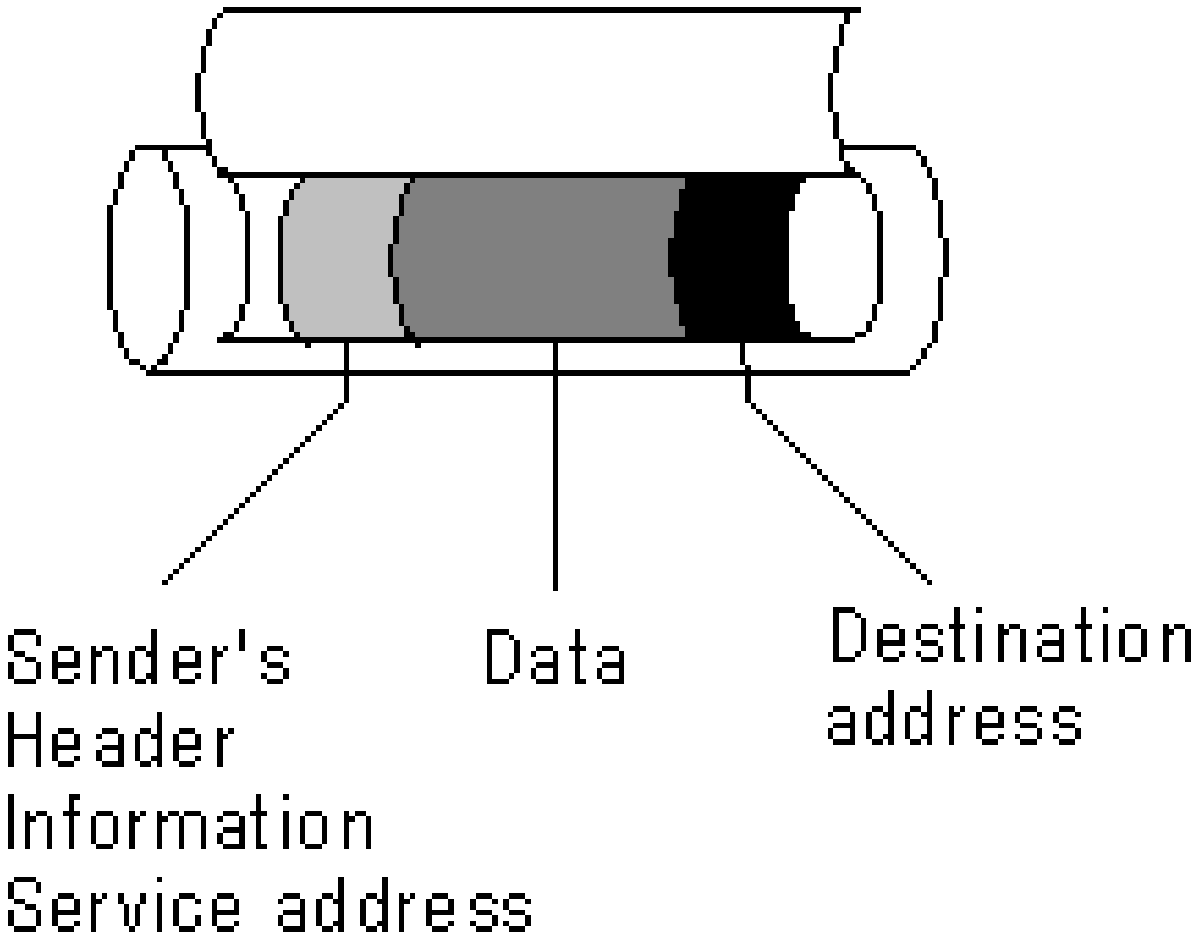
Přenos dat v síti

- Data se v síti přenáší za využití:
  - Paketů
  - Nespojované komunikace
  - Síťových protokolů (TCP/IP)
  - IP adresace

Paket

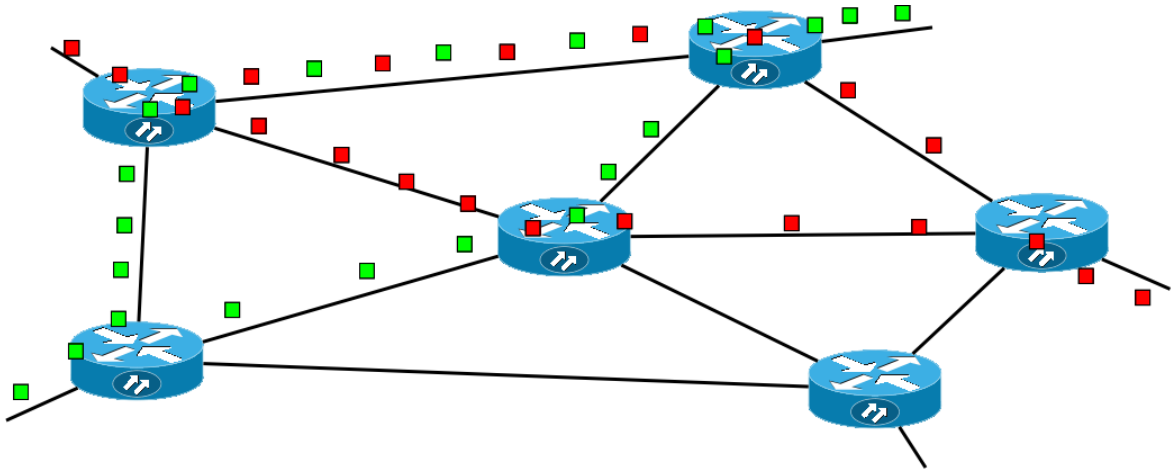
- základní přenosová jednotka (alespoň v sítích TCP/IP). Skládá se z dat a metadat.
- Obsahuje záhlaví informace k přenosu a případně zápatí.
- ***Metadata** - jsou strukturovaná data o datech. Příkladem je katalogizační lístek v knihovně, obsahující data o původu a umístění knihy: jsou to data o datech v knize, uložená na katalogizačním lístku.

Packet

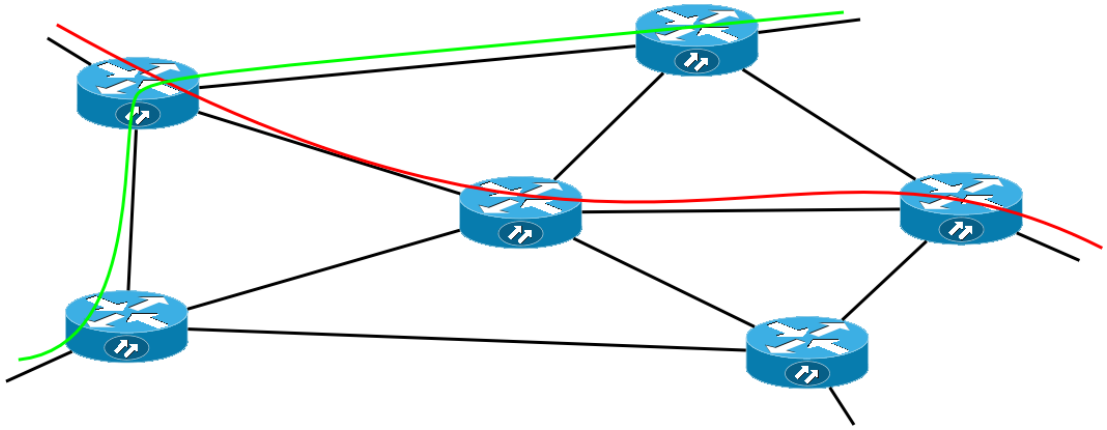

Sender's
Header
Information
Service address
Data
Destination
address

Nespojovaná komunikace

- Komunikaci mezi dvěma entitami není vytvářený rezervovaný okruh (spoj), ale data jsou rozdělena na malé části — tzv. pakety,
- Pakety jsou přenášené sítí nezávisle na sobě
- Takovýto transport dat je také odolnější vůči výpadkům, v případě poškození, či přetížení jedné cesty lze dynamicky přesměrovat pakety jinudy aniž by se narušila vlastní komunikace.
- Nevýhodou je komplikovanější řízení provozu takovéto sítě — je nutné řešit směrování **každého paketu v síti k jeho cíli**.



Nespojovaná komunikace



Spojovaná komunikace

Komunikační protokoly

- Přesně definují způsob, jakým probíhá komunikace realizující konkrétní funkci a to na všech úrovních.

- Máme protokoly pro zasílání dat, navazování zabezpečených kanálů, vyhledání síťové adresy odpovídající doménovému jménu, doručení emailu atd.
- Protokol je známý oběma komunikujícím stranám a popisuje přesně *jaký obsah, v jakém pořadí a s jakým časováním* je předáván. Odklon od takto strukturované komunikace je možné interpretovat jako chybu.

TCP/IP

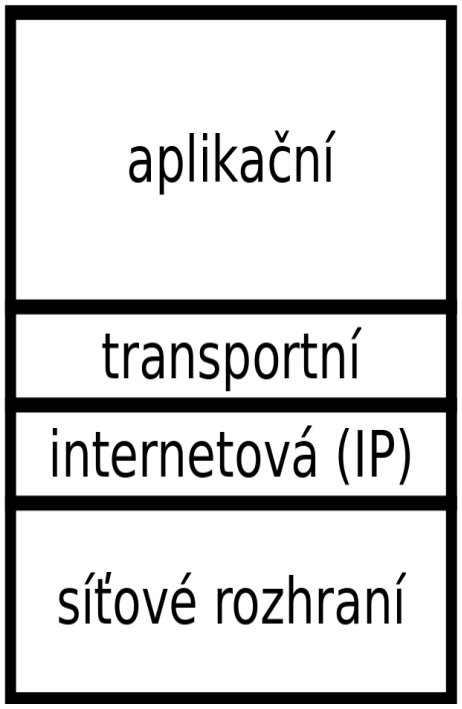
- Základním principem prostupujícím architekturu počítačových sítí je rozdělení komunikace do vrstev podle abstrakce. Každá vrstva je zodpovědná za popis přenosu od úrovně aplikace až po komunikaci po fyzických spojích. Síťový model TCP/IP je základním kamenem všech dnešních sítí a i celého internetu a je pojmenován podle dvou hlavních protokolů zajišťujících směrování a transport dat mezi uzly.

TCP/IP

- Rodina protokolů TCP/IP předpokládá existenci čtyř vrstev:
  - - aplikační vrstvy
  - - transportní vrstvy
  - - síťové vrstvy
  - - vrstvy síťového rozraní

TCP/IP

Vrstvy:



- **Aplikační** - zahrnuje protokoly síťových aplikací: elektronické pošty, HTTP, www, ftp…
- **Transportní** - tato vrstva zajistí spolehlivost a celistvost dat
- **Síťová (internetová, IP vrstva)** - Protokol IP popisuje adresaci uzlů, rozklad dat na pakety a jejich směrování uvnitř sítě.
- **Síťové rozhraní** – zajišťuje komunikaci po fyzickém médiu (kabelu) a přenos dat mezi dvěma přímo spojenými stanicemi

Jak to začalo jak to funguje…

- https://www.youtube.com/watch?v=vDrUUqHsyok

IP adresace

- **IP adresa určuje jednoznačně počítač v síti**

- Adresa je zleva hierarchická, to znamená, že adresné prostory jsou přidělovány fixací čísel od leva: například Masarykova Univerzita má k dispozici rozsah
  147.251.0.0 - 147.251.255.255.
- Některé adresní rozsahy jsou vyhrazené speciálním účelům, například pro privátní podsítě, které nejsou adresovatelné zvenčí jsou vyhrazené následující rozsahy:

- Vzhledem k rostoucímu počtu připojených zařízení došlo v roce 2011 k vyčerpání adresného prostoru 32 bitů. Z toho důvodu je zaváděn nástupný protokol IPv6, který k adresaci využívá 128 bitů a zapisuje se v hexadecimálních oktetech, například adresa 2001:4860:b002::68 odpovídá testovací adrese ipv6.google.com.

IP adresy vs. domény

- IP adresy používané pro adresaci strojů v síti nejsou vhodné pro koncové uživatele — špatně se pamatují, lze je snadno zaměnit a mohou se měnit. Proto se používá jmenná služba, která popisuje stroje pomocí textových jmen rozdělených do domén.

IP vs. domény

.cz = 1. řád (koncovka)
example.cz = 2. řád
blog.example.cz = 3. řád (subdoména)
www.blog.example.cz = 4. řád

- Domény nejvíce vpravo označujeme jako domény nejvyššího řádu: jedná se o národní domény a obecné domény jako .net, .com, .org a další. Jejich registrace a delegace správy spadá pod mezinárodní organizaci ICANN.

- Například českou doménu .cz spravuje sdružení CZ.NIC (nic.cz), které mimo jiné prostřednictvím tzv. registrátorů registruje domény nižšího řádu — například muni.cz. Vlastník určité domény může libovolně vytvářet a spravovat domény nižších řádů, v kompetenci MU je tedy správa domén jako is.muni.cz, phil.muni.cz…

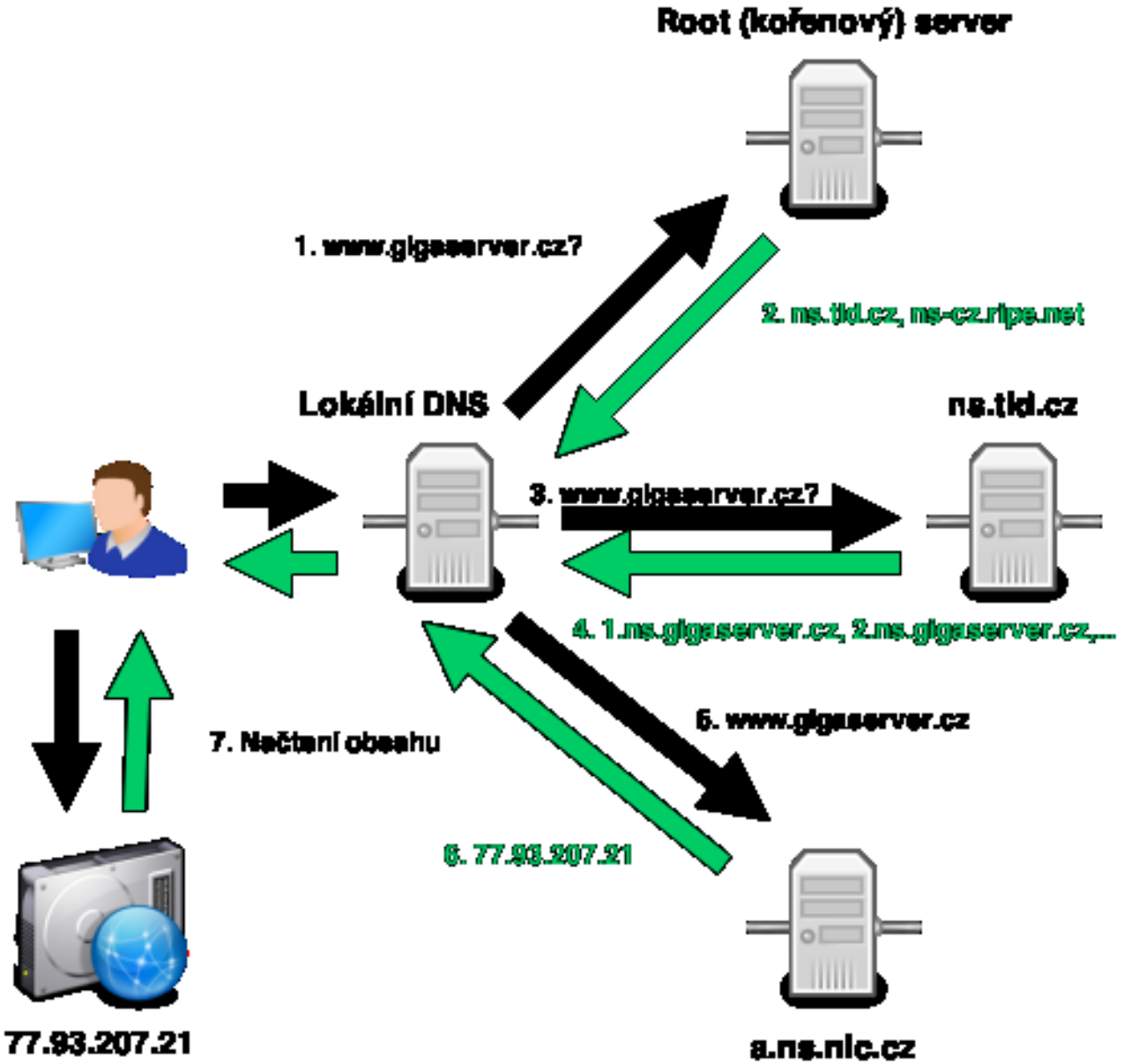
IP vs. domény

- Pro překlad z doménových jmen na IP adresy se používá Domain Name System (DNS). Například:

- muni.cz. -> 147.251.5.231 Tento protokol postupuje od domény nejvyššího řádu a dotazuje se příslušných DNS serverů na adresy zodpovědné za domény nižšího řádu tak dlouho, než dostane informaci o stroji, na který směřuje doména nejnižšího řádu přítomná v názvu.

Jak domény fungují ?

- 1. Uživatel zadá název domény do prohlížeče a lokální DNS server se obrátí na některý kořenový server a zeptá jestli nezná IP adresu domény www.gigaserver.cz.
- 2. Kořenový DNS server nezná IP adresy konkrétních domén, ale ví na kterých serverech se nachází záznamy .CZ domény a pošle lokálnímu DNS seznam těchto serverů.
- 3. Lokální DNS se tak obrátí na servery, které záznamy o .CZ doménách obsahují (ns.tld.cz, ns-cz.ripe.net,...).
- 4. Tyto servery však stále konkrétní IP adresu neznají, ale mají informace o všech .CZ doménách II. řádu a tak lokálnímu DNS odpoví názvy serverů, které informaci o IP adrese budou mít.
- 5. Lokální DNS se tak obrátí na tyto servery (1.ns.gigaserver.cz, 2.ns.gigaserver.cz, 3.ns.gigaserver.cz, 4.ns.gigaserver.cz).
- 6. DNS server konktrétní IP adresu požadované domény zná, je to 77.93.207.21 a pošle ji zpět lokálnímu DNS.
- 7. Lokální DNS pak předá IP adresu počítači uživatele, ten se spojí s daným server a zobrazí obsah požadované domény.



- Zdroj: https://kb.gigaserver.cz/co-je-to-ip-adresa-jak-funguje-dns/

Služby sítě internet

- Hlavní služby poskytované sítí internet:
  - WWW
  - E-mail
  - E-banking
  - Cloudové služby
  - VoIP (hlasové služby)
  - FTP
  - Peer-to-peer (P2P)

WWW (Word Wide We

- Multimediální obsah, poskytovaný uživatelům pomocí protokolu HTTP -> primárně webové stránky

- Uživatelé tento obsah konzumují pomocí webových prohlížečů a v podstatě se stal synonymem pro internet jako takový.

E-mail

- Již od raných dob internetu je k dispozici zasílání textových zpráv mezi jednotlivými uživateli, dodnes je zajišťován pomocí protokolu SMTP, který byl vyvinut v 70. letech.

- 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 (off-line) přistupovat (vybírat zprávy)

- Alternativou ke stahování pošty je využití některého z webmailů, což jsou v podstatě webové aplikace umožňující vzdálenou manipulaci s emailovou schránkou. Služba jako taková negarantuje pravdivost údajů o odesílateli, ani žádné další bezpečnostní prvky (šifrování), ty je nutné zajistit použitím příslušného software na obou komunikujících stranách.

E-banking

- Internetové bankovnictví umožňuje provádět pomocí síťové infrastruktury finanční transakce. Jedná se v jádru o zprostředkování zabezpečené komunikace mezi uživatelem a jeho bankou, při které je ověřena uživatelova identita a přijat příkaz k provedení dané operace.

- K zajištění dostatečného zabezpečení se kromě obvyklého https spojení a uživatelského jména a hesla užívá i tzv. vícestupňového ověření — např zaslání potvrzujícího kódu pomocí SMS. Zvyšuje se tak obtížnost zneužití ukradených přístupových údajů případným útočníkem. Pro usnadnění mezinárodních transakcí a zvýšení důvěry na straně prodejců i nakupujících vznikly tzv. zprostředkovatelské služby — jako například PayPal — tyto zjednodušují provádění online transakcí a zvyšují jejich bezpečnost (obchodník například nepřijde do styku s číslem platební karty zákazníka a pod.).

Cloud

- Poskytování služeb či programů uložených na serverech na Internetu s tím, že uživatelé k nim mohou přistupovat například pomocí webového prohlížeče a používat je prakticky odkudkoliv.

- Uživatelé neplatí (za předpokladu, že je služba placená) za vlastní software, ale za jeho užití. Nabídka aplikací se pohybuje od kancelářských aplikací, přes systémy pro distribuované výpočty, až po operační systémy provozované v prohlížečích, jako je například eyeOS či iCloud.

- Příklady: Google docs, dropbox, google drive…

Cloud

VoIP (hlasové služby)

- technologie, umožňující přenos digitalizovaného hlasu v těle paketů rodiny protokolů TCP/IP prostřednictvím počítačové sítě
- Využívá se pro telefonování prostřednictvím Internetu nebo intranetu
- Nutnou podmínkou pro srozumitelné a spolehlivé VoIP telefonní spojení je zajištění tzv. kvality služby, zkráceně označované QoS.

- **QoS** - nastavení aktivních prvků (např. routeru) sítě tak, aby upřednostňovaly hlasová data před ostatním provozem. Na většině domácích routerů lze nastavit prioritu hlasového (nebo videokonferenčního) datového toku tak, aby ostatní uživatelé sdílející tutéž linku nemohli nezahltit její kapacitu například stahováním objemných dat.

- **Příklady:** Skype, Google hangouts

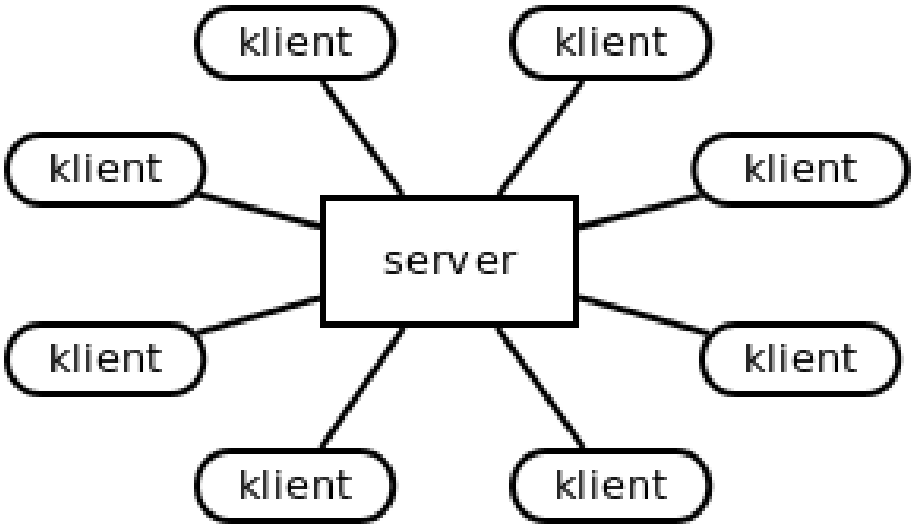
FTP- File Transfer Protocol

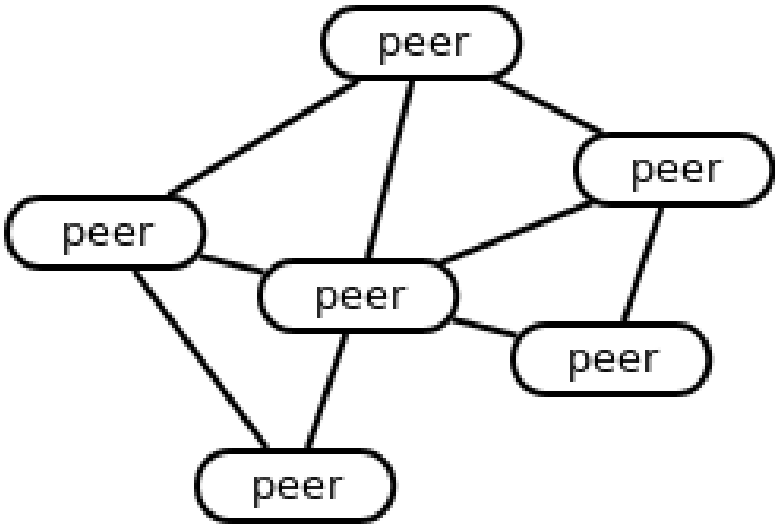
- Klasický protokol pro přenos souborů po síti
- Umožňuje navázat spojení se vzdáleným počítačem, procházet danou adresářovou strukturu **(složky)** a přenášet soubory oběma směry.
- Zpravidla chráněn uživatelským jménem a heslem. Provoz po FTP není nijak šifrován, proto pokud je to možné je vhodné používat zabezpečenou variantu FTPS (obdoba HTTPS). V dnešní době se s tímto protokolem uživatel setká nejčastěji při přístupu na webhostingové diskové prostory, případně na vnitřní firemní sdílená datová úložiště.

- **Vhodné programy:** Total Commander, FileZilla….

Peer-to-peer (P2P)

- Většina služeb funguje na bázi **klient-server**





- U klient-server dochází k distribuci obsahu uloženého na serveru ke klientům, klienti navzájem si data nepředávají. => Velká zátěž na serveru, data pouze na něm
- Pokud server selže, žádný klient svá data neobdrží

P2P

- P2P odstraňují výsadní pozici serveru a jsou založené na decentralizované a distribuované architektuře.
- Každý peer je tak zároveň klientem i serverem: poskytuje služby ostatním peerům a zároveň využívá jejich služeb

P2P

- **Výhody:** rozložení zátěže mezi peery (oproti její koncentraci na straně serveru), zvýšené odolnosti vůči výpadku a dobrou škálovatelnost (lze libovolně navyšovat počet peerů, aniž by se přetížil centrální server).
- **Nevýhody:** náročné vystavění p2p sítě (složitější modely komunikace) a nepřehlednost správy takovéto sítě.
- **Příklady**: Skype, bitttorent

Konfigurace síťových služeb

- Vybrané konfigurační prvky:
  - Zabezpečená wifi
  - DHCP, statická IP
  - VPN
  - Eduroam
  - Firewall

Zabezpečená Wifi – viz přednáška o kryptografii

- Při konfiguraci bezdrátového připojení je nezbytné dbát na co největší míru zabezpečení.
- Bezdrátový přenos je možné odposlouchávat a následně zneužít.
- K šifrování nabízí většina přípojných bodů pro domácnosti dvojí volbu: **WEP a WPA**. WEP protokol je od roku 2004 považován za **zastaralý** a lze jej běžně dostupnými prostředky prolomit. WPA (a jeho novější varianta WPA2) používají pro silnější algoritmy s dynamicky měněným klíčem, což zamezuje získání klíče dlouhodobým odposlechem.

DHCP a statická IP

- Každé zařízení připojené do počítačové sítě musí mít přidělenu jednoznačnou IP adresu.
- **Je v podstatě dvojí možnost, jak adresy v síti rozdělovat:**

- 1) Staticky-zde je třeba o novou adresu požádat správce sítě a následně ji na příslušných místech v nastavení systému zadat.

- 2) DHCP - adresa je přidělována automaticky DHCP serverem přítomným v síti (např. v domácnostech součástí routeru) bez dalších zásahů uživatele. Takto přidělená adresa se navíc může měnit při každém připojení do sítě.

VPN – Virtuální privátní síť

- Slouží k vytvoření zabezpečeného propojení fyzicky vzdálených počítačů tak, jakoby byly propojeny lokální sítí.
- Umožňuje tak například vzdálené připojení do firemní sítě, nebo propojení vzdálených poboček do jedné sítě při zachování vysoké úrovně zabezpečení.
- V rámci univerzity je VPN také k dispozici a umožňuje například přístup do elektronických zdrojů (placené články…) tak jako by se stroj připojoval z univerzitní sítě (jako by byl třeba zde v učebně).
- Podrobné návody k navázání připojení jsou dostupné zde: http://vpn.muni.cz

Eduroam

- Eduroam je mezinárodní projekt umožňující studentům a zaměstnancům univerzit připojení do bezdrátových sítí všech zúčastněných institucí.

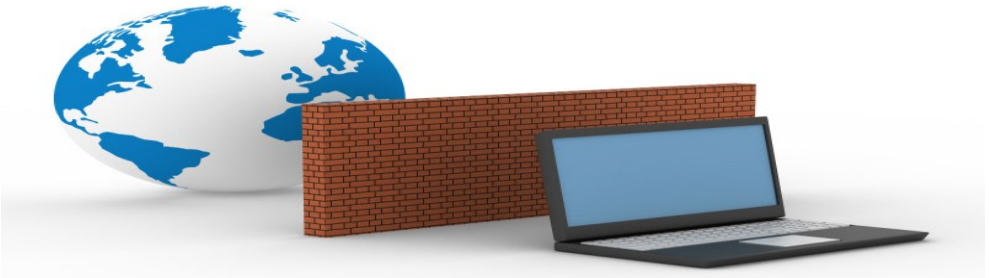
- Jedná se o příklad federativního autentizačního mechanizmu, kdy je uživateli umožněno se přihlašování do libovolné zapojené sítě prokazovat přihlašovacími údaji své domovské instituce (UČO, sekundární heslo).

- Tato služba velmi usnadňuje připojení nejen na Masarykově univerzitě (na všech fakultách stejné nastavení), ale především při návštěvách jiných institucí — zapojené jsou nejen univerzity, ale například i veřejné knihovny, instituty AV a další. Návody jsou opět k dispozici na http://eduroam.muni.cz

Firewall

- **Firewall** je virtuální nástroj oddělující provoz mezi sítí (internetem) a počítačem, tak že propouští jedním nebo druhým směrem informace podle předem definovaných pravidel. Brání tak zejména před neoprávněným vniknutím do sítě a odesílání dat bez vědomí a souhlasu uživatele či oprávněné osoby. Ve virtuálním prostředí domácností i firem je instalace brány firewall nejefektivnějším a nejdůležitějším krokem při ochraně a zabezpečení počítače.

- Firewall definuje pravidla, podle kterých může probíhat komunikace mezi počítači či sítěmi, resp. povolí se podmínky a služby, které jsou nutné pro provoz a ostatní jsou zakázány. Firewall nepřetržitě kontroluje dění v domácí či firemní síti a podrobně jej monitoruje. Informuje i o legálních procesech, vzniklých použitím některých aplikací a dovolí tuto činnost povolit či zablokovat.



Děkuji za pozornost