3 KOMUNIKACE, SÍTĚ

RYCHLÝ NÁHLED KAPITOLY

Tato kapitola obsahuje seznámení se základními službami, dále objasní principy internetu a s tím související základy komunikace v síti včetně protokolů a základních příkazů (ipconfig, tracert, ping, arp) sloužících k zjištění dostupnosti zdroje na Internetu. Budou objasněny pojmy související s DNS serverem, maskou, bránou. Tyto znalosti jsou aplikovatelné pro vzdálenou správu, komunikační služby a v rámci služeb pro přenos a publikaci hypertextů založené na http protokolu (www).

CÍLE KAPITOLY

Cílem kapitoly je seznámit studenty se základními pojmy, se kterými se setkají při práci s Internetem, jako rozsáhlou sítí počítačů. Studenti po prostudování textu budou schopni identifikovat síťové prostředí a základní problémy v komunikaci v rámci Internetu

ČAS POTŘEBNÝ KE STUDIU

V této kapitole je vhodné si uváděné příkazy prakticky odzkoušet. Z tohoto důvodu je čas potřebný ke studiu v rozsahu 2-5 hodin, podle míry praktické práce.

KLÍČOVÁ SLOVA KAPITOLY

Počítačová síť, TCP/IP protokol, ISO/OSI model, maska sítě, brána, IP adresa, služby Internetu, komunikace

3.1 Principy komunikace v sítích

Pro komunikaci (jakoukoliv, ne pouze počítačovou), je nutné zajistit, aby systémy byly kompatibilní, aby komunikovaly podle jednotných pravidel. Pro funkční komunikaci, musí být stanovena jednoznačná pravidla. Tato pravidla jsou dána komunikačním protokolem

(můžete srovnat například s „protokolem společenským“, „hradním protokolem“ apod., definujícími chování ve společnosti či v prezidentské kanceláři).

Komunikační protokol musí jednoznačně ošetřit všechny stavy, ke kterým může v počítačové síti dojít a musí být schopen zabezpečit komunikaci. Komunikační protokol je množina pravidel, která určují syntaxi a význam jednotlivých zpráv při komunikaci. Je zřejmé, že musí být univerzální, zejména s ohledem na rozmanitost počítačových systémů komunikujících v prostředí Internetu, počínaje různými operačními systémy (Windows, Linux, IOS, Android apod.), různých hardwarových platforem (PC, Apple, tablety, Smartphone apod.), či nepřeberným množstvím komunikujícího software atd.

3.1.1 KOMUNIKAČNÍ PROTOKOLY

Je tedy zřejmé, že nastavení komunikačního protokolu je zásadní a podstatná věc, která zabezpečuje komunikaci a funkčnost služeb v síti, potažmo v Internetu. Porovnejme nejdříve prostředí, se kterým se setkáte na OPF. Příklady jsou opět zjednodušené, slouží pro pochopení principů.

IPX/SPX

Každý student OPF má účet Novell, prostřednictvím kterého se přihlašuje do fakultní sítě. V této síti má k dispozici přidělené prostředky (disk L, disk K apod. tiskárny) a přidělená práva (na disku L může zapisovat, mazat, vytvářet adresáře, na disku K může prohlížet obsah, na vybraných tiskárnách může tisknout apod.). Do sítě se student přihlašuje svým jménem a heslem, aby uživatel mohl v síti pracovat, musí mít vytvořený účet s právy.

Jedná se tedy o síť centrálně spravovanou, autentizace je na úrovni uživatelů a prostředků vytvářených správcem. Tato síť funguje na protokolu IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) což je sada protokolů používaná síťovým operačním systémem Novell NetWare a používá se zejména pro komunikaci typu klient/server[8].

Výhodou takovéto sítě je bezpečnost a organizovanost, nicméně použití této sítě jako základu Internetu by bylo nereálné, protože by každý uživatel musel mít přihlašovací údaje a práva k přiděleným prostředkům.

NetBIOS

Jiný typ sítě, se kterým se studenti na OPF setkávají, je síť Microsoft. Tato síť je založena na protokolu NetBIOS (resp. NetBEUI - NetBIOS Extended User Interface). Protokol je určen především pro komunikaci v malých lokálních sítích, způsob adresování nepodporuje routování. Není tedy možné spojit více sítí bez nutnosti použití brány. Zjednodušeně

[8] Architektura klient/server je blíže popsána v kapitole 4

se dá říct, že každý uživatel rozhoduje o prostředcích, které nabídne ostatním a přiděluje jejich práva. Počítač je v síti identifikovaný jménem, může být vázaný na skupinu počítačů. Základním problémem je nekoordinovanost při přidělování jména počítače, kdy jméno je přidělováno při instalaci operačního systému. V síti potom může docházet k nejednoznačnosti v názvech počítačů, kdy více počítačů má shodný název („doma“, „mamka“, „Jirka“ apod.). V dnešní době tento protokol nemá větší využití, nicméně slouží většinou ke sdílení tiskáren a souborů v síti menšího rozsahu. Protokol je charakteristický vysokou přenosovou rychlostí a jednoduchostí konfigurace. NetBEUI v současnosti umožňuje pracovat nad protokolem TCP/IP, čímž dochází k rozložení komunikace mezi tyto protokoly a zefektivnění síťového provozu.

Tento protokol by byl z pohledu správy sítě pro Internet vhodný, nevyžaduje centrální správu, uživatelé rozhodují o tom, co nabídnou ostatním. Je však zcela nepoužitelný z důvodu nekoordinovaného přidělování jmen počítačů[9] a malé bezpečnosti.

TCP/IP

V dnešní době použití IPX/SPX a NetBIOS značně kleslo, díky univerzálnosti TCP/IP protokolu, (Transmission Control Protocol / Internet Protocol – „primární přenosový protokol/protokol síťové vrstvy“), který obsahuje sadu protokolů pro komunikaci v počítačové síti. Síťová komunikace je rozdělena do tzv. vrstev. Výměna informací mezi vrstvami je přesně definována. Každá vrstva využívá služeb vrstvy nižší a poskytuje své služby vrstvě vyšší.

V rámci tohoto protokolu je adresace prováděna na úrovni síťového rozhraní prostřednictvím IP adresy. Přidělování této adresy je vázané pravidly, část adres je přidělována, část může být distribuována libovolně (obdobně jako jméno počítače v síti Microsoft) za dodržení určitých pravidel. V současnosti existuje TCP/IP ve verzi 4 a 6. V těchto skriptech se z důvodu snazšího pochopení zaměříme na IP verze 4.

V současnosti je tedy nutné, aby každý počítač, který chce přistupovat do sítě internet, komunikoval pomocí protokolu TCP/IP.

3.2 Konfigurace připojení

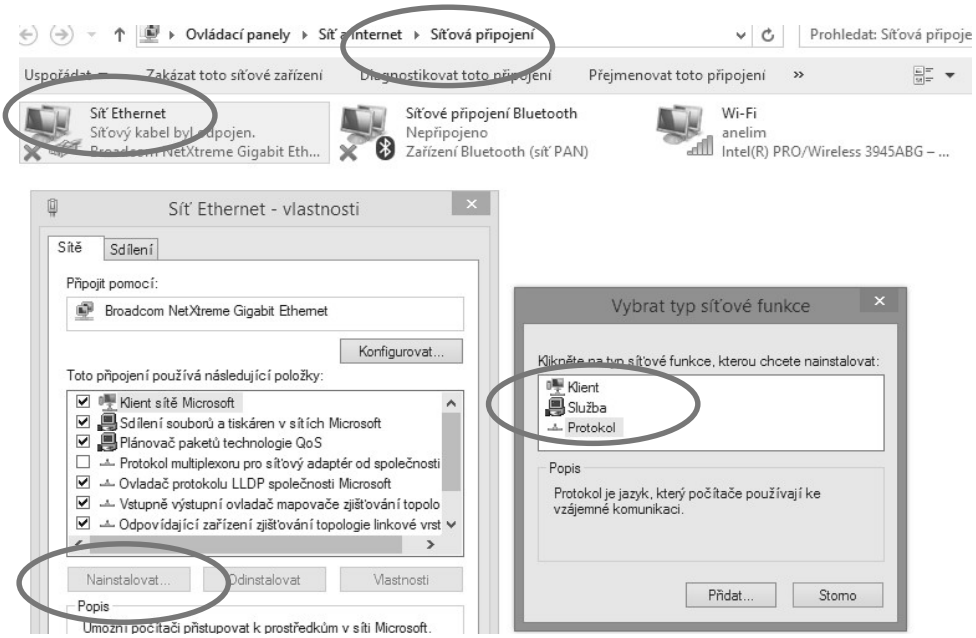
Volbu protokolu, služeb a klientských aplikací v prostředí Windows[10] provádíme v Centru síťových připojení, v nastavení adaptéru vybereme příslušné síťové rozhraní a ve vlastnostech můžeme nastavit parametry připojení.

Základní parametry[11], pro které musíme při použití TCP/IP protokolu upřesnit nastavení jsou:

- IP adresa počítače
- Síťová maska (Net Mask)

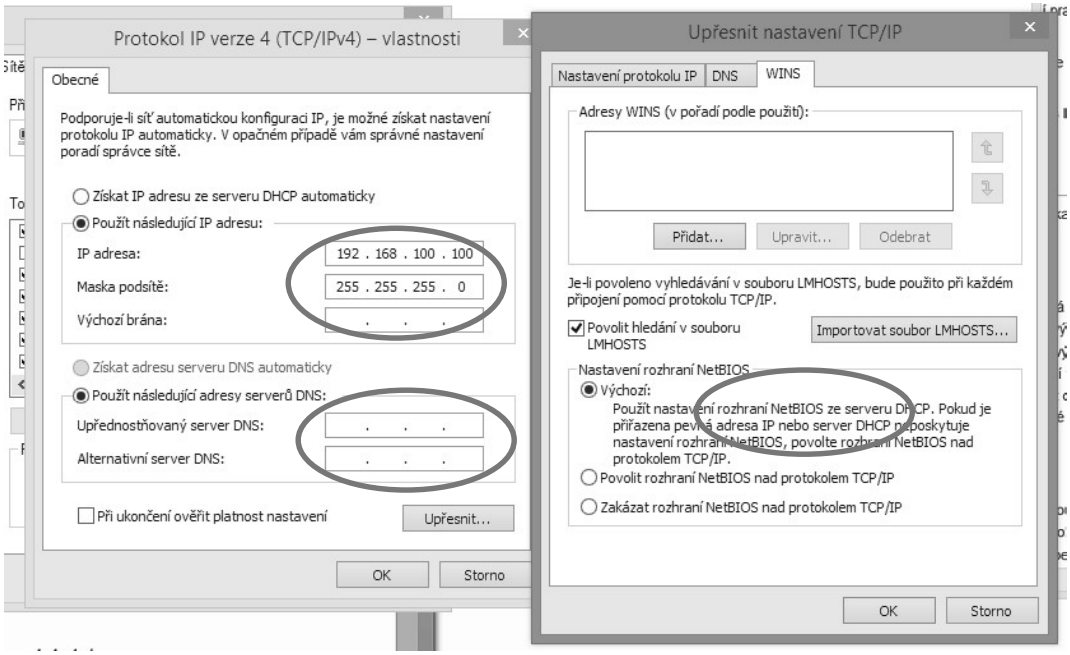
[9] Účelově zjednodušeno na základě peer to peer sítě Microsoft
[10] Vzhledem k softwarovému vybavení učeben OPF a dominantnímu postavení tohoto operačního systému v segmentu PC uvádíme příklady nastavení v OS Windows
[11] Převzato s úpravami z http://www.gvp.cz/local/new/ucebnice/vyptech/internet/tcpip.htm

- Výchozí brána (Default Gateway)
- IP adresa Domain Name Serveru (DNS
- IP adresa Domain Name Serveru (DNS)



Obrázek 22: Nastavení síťových připojení v MS Windows

Zdroj: Vlastní zpracování



Obrázek 23: nastavení IP adresy, masky, brány a DNS, povolení NetBIOS

Zdroj: Vlastní zpracování

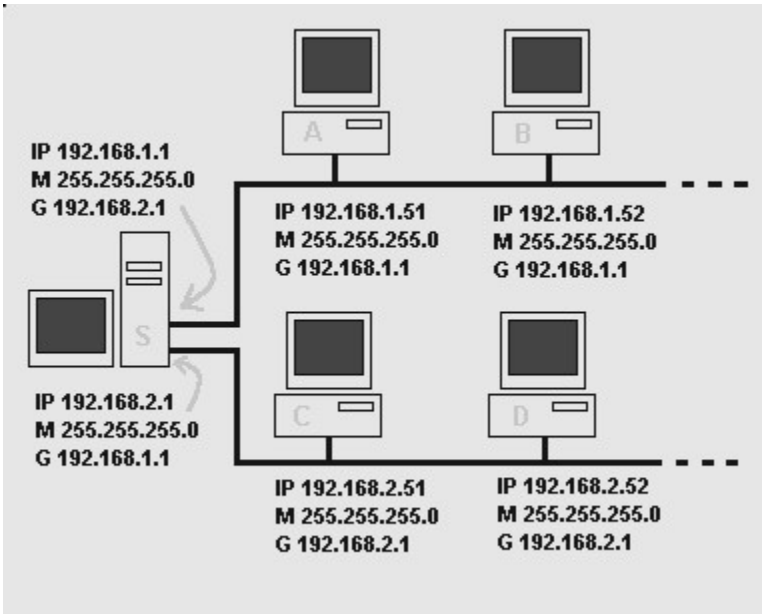
Nastavení může provádět buď uživatel, je-li povolena DHCP služba, lze použít vzdálenou konfiguraci prostřednictvím DHCP serveru.

IP adresa verze 4 je čtyřbajtové číslo, které identifikuje síťovou kartu počítače v rámci protokolu TCP/IP. Zapisuje se ve formátu čtyř čísel oddělených tečkou např.: 192.168.100.1. Rozsah je od 0.0.0.0 do 255.255.255.255. Tato čísla přiděluje správce systému podle pokynů organizace IANA (Internet Assigned Numbers Authority).

Internet je spojením mnoha menších místních a regionálních sítí. Tyto sítě jsou propojeny pomocí bran (Gatway). Brána je hardwarový prostředek (např. počítač), který obsahuje více síťových rozhraní, propojuje více sítí a předává data mezi těmito sítěmi.

Net Mask (síťová maska), určuje rozmezí adres, které patří do místní sítě. Opět zjednodušeně, maska obsahuje hodnoty 255 nebo nula, IP adresy, které se shodují na pozicích, kde je v síťové masce nula (přičemž nuly se doplňují postupně zprava), patří do stejné místní sítě[12]. Má-li počítač nastavené IP=194.168.1.1 a Net Mask=255.255.255.0, všechny adresy začínající 194.168.1. patří do stejné lokální sítě. Na posledním místě mohou mít cokoliv. Pokud má PC v lokální síti komunikovat s PC mimo tuto síť, komunikuje prostřednictvím brány.

Na obrázku je znázorněna situace, kdy počítač označený S propojuje síť 192.168.1.* se sítí 192.168.2.*



Obrázek 24: Brána počítačové sítě

Zdroj: [online]. [vid. 1.9 2013]. Dostupné z: http://www.gvp.cz/local/new/ucebnice/vyptech/internet/tcpip.htm

[12] Velmi zjednodušený příklad, ve skutečnosti maska může mít i jiné hodnoty, které definují rozsah a počet povolených adres, toto je však obsahem jiných předmětů.

Síť na obrázku je složena ze dvou podsítí (místních sítí). Pokud chce počítač A komunikovat s počítačem B, na základě znalosti obou IP adres a své síťové masky zjistí, že počítač B je ve stejné podsíti a proto mu může poslat zprávu přímo.

Když chce počítač A komunikovat s počítačem C, na základě znalosti IP adres a síťové masky zjistí, že počítač C není ve stejné podsíti a proto směruje svou komunikaci na bránu (tedy na komunikaci směrem z podsítě ven). Brána zabezpečí komunikaci s druhou podsítí, tedy s počítačem C.

DNS - Domain Name Server (Domain Name System, Domain Name Services) zajišťuje překlad číselných IP adres na doménové adresy. Např. www.opf.slu.cz = 193.84.209.5. Každý počítač musí znát DNS, jinak by nemohl používat adresaci pomocí doménových adres. Pokud nezná PC adresu DNS serveru, může komunikovat pomocí IP adres, nemůže komunikovat pomocí doménových adres. Fungují tedy základní služby Internetu. IP adresa DNS serveru i IP adresa počítače může být přidělována vzdáleně prostřednictvím DHCP.

3.2.1 PŘÍKAZOVÝ ŘÁDEK A ZÁKLADNÍ PŘÍKAZY

Pro základní práci s protokolem TCP/IP a kontrolu funkčnosti komunikace můžete použít příkazů zadávaných v tzv. příkazovém řádku (podle verze OS se jedná o příkaz CMD, command apod.). Příkazy se zadávají ve tvaru ***PŘÍKAZ***, ***mezera***, ***oddělovač***, ***parametry***. Oddělovačem je znak „-„ nebo „/“. Parametrů (atributů) může být více. Parametr „?“ zobrazí nápovědu k příkazu. V prostředí Windows nezáleží na velikosti znaků (malá, velká písmena).

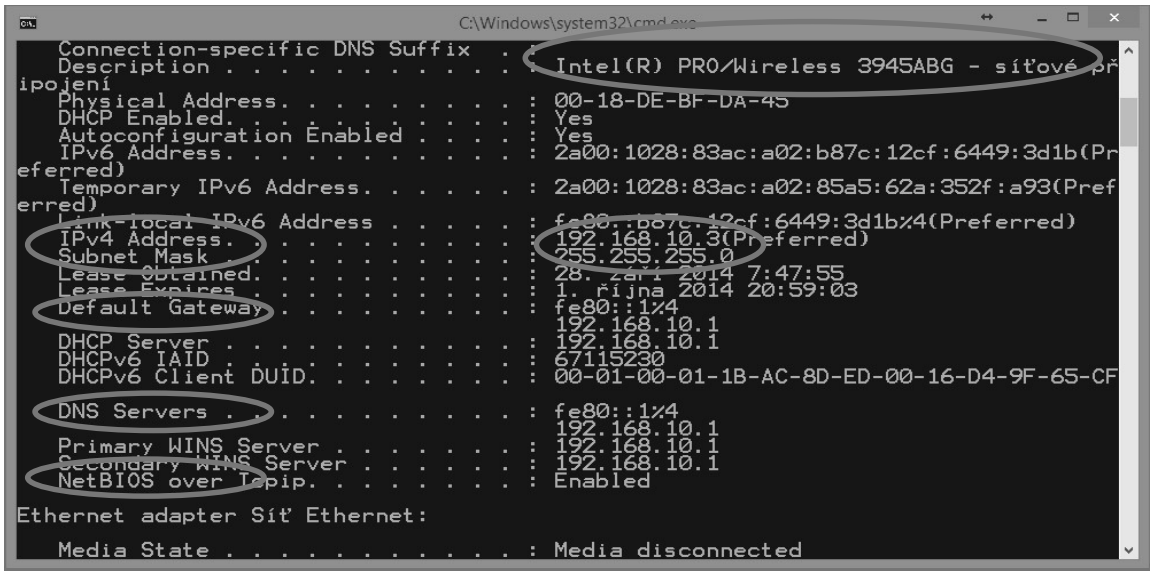
Například příkaz ***ping -4 www.volny.cz*** má parametr „4“, který udává, že se má pracovat s IP adresami verze 4. Příkaz zkouší dostupnost adresy www.volny.cz.

- ***Ipconfig*** - vypíše aktuální konfiguraci TCP/IP počítače, nastavení všech adaptérů dostaneme použitím příkazu ipconfig /all.
- ***Ping*** – příkaz ***ping adresa*** (IP nebo doménová) vyšle k zadanému počítači požadavek na odpověď a vypíše, zda a za jak dlouho je tento počítač dostupný a kolikrát přešla komunikace přes aktivní síťový prvek (router).
- ***Tracert*** - funguje podobně jako Ping, ale navíc vypisuje i všechny brány, kudy zpráva prošla.
- ***Nslookup*** – příkaz zjišťující IP adresu na základě DNS

Následující obrázek ukazuje výpis příkazu ***ipconfig /all***.

Na výpisu je vidět používané síťové adaptéry (Intel Wireless), fyzická adresa adaptéru a přidělené IP adresy verze 6 a 4.dále je zobrazena maska a adresa brány a DNS serveru.

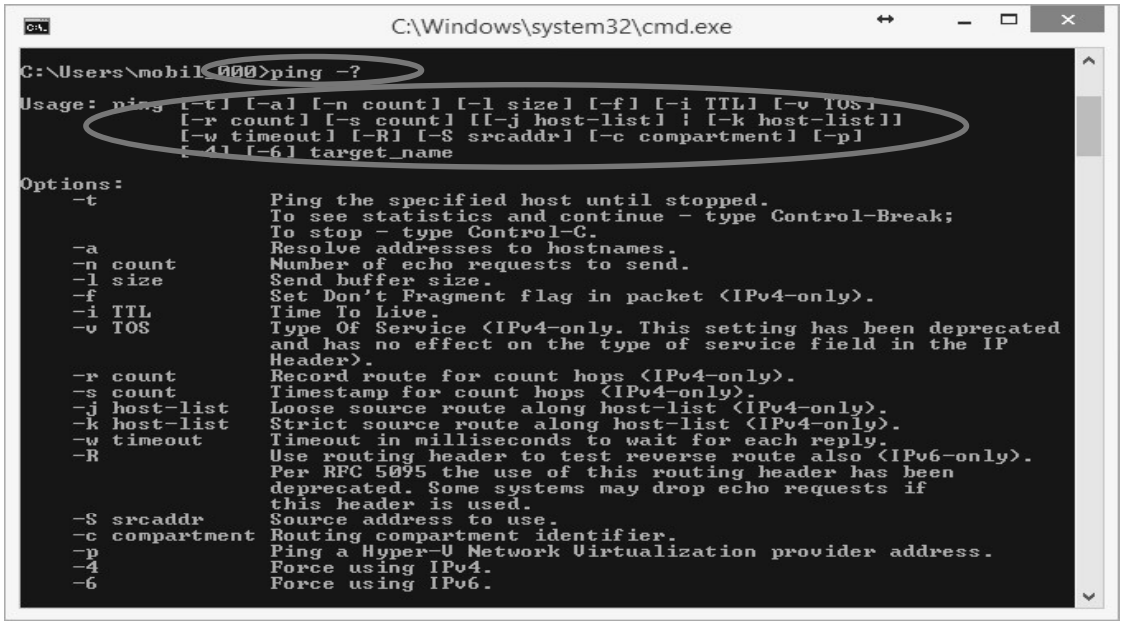
Rovněž je zřejmé, že kooperuje TCP/IP protokol a NetBIOS.



Obrázek 25: Výpis nastavení síťového adaptéru příkazem ipconfig

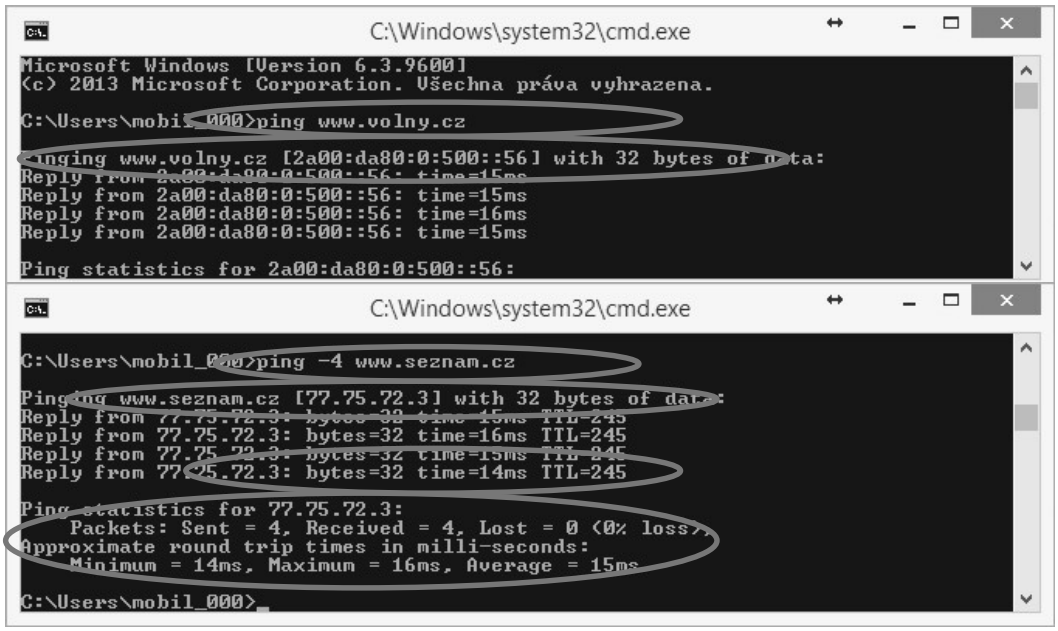
Zdroj: Vlastní zpracování

Parametry (atributy) jednotlivých příkazů můžeme vypsat pomocí parametru „?“. Pokud je parametr vyžadován, vypíše se seznam parametrů u některých příkazů i při zadání příkazu bez uvedení požadovaných parametrů.



Obrázek 26: Parametry příkazu ping

Zdroj: Vlastní zpracování



Obrázek 27: Příkaz ping

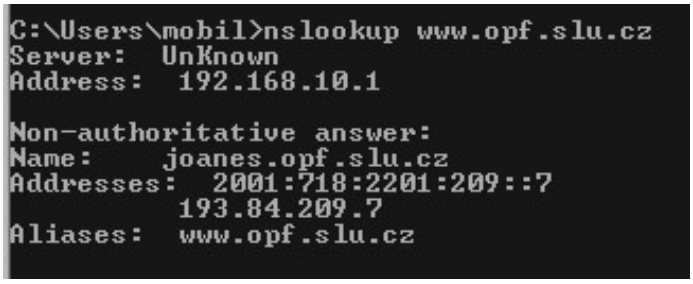
Zdroj: Vlastní zpracování

Předchozí obrázek ukazuje výpis příkazu ping, v prvním případě bez parametru. Je zjišťována dostupnost počítače s doménovou adresou www.volny.cz a www.seznam.cz. Pokud zadáme příkaz s parametrem „4“ vypíše se IPv4, jinak IPv6(pokud je dostupná). Protože je dostupný DNS server, dojde k překladu na IP adresu (u verze IPv4 77.75.72.3). Současně se vypíše čas dostupnosti a životnost dat (datagramu) která je dána hodnotou TTL (zjednodušeně, čím vyšší hodnota TTL tím delší čas má příkaz na nalezení hledaného počítače (Hodnota udává počet povolených přechodů přes aktivní síťové prvky. Že je doménová adresa v podstatě „převlečenou“ IP adresou si můžeme ověřit tak, že zjištěnou IP adresu zadáme jako adresu stránky do prohlížeče.

Obrázek 28: IP adresa zadaná do prohlížeče

Zdroj: Vlastní zpracování

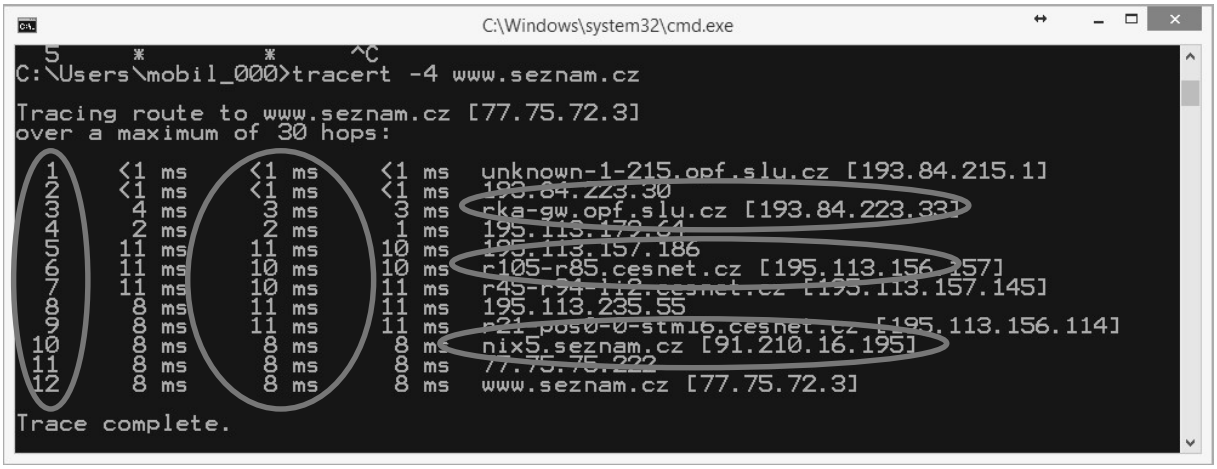
Jak bylo zmíněno, počítač při směrování požadavků nemůže znát doménové adresy, ty se evidují na tzv. DNS serverech. Počítač, zjednodušeně řečeno netuší, jakou IP adresu ve skutečnosti má například počítač, na kterém je provozován www server s doménou www.opf.slu.cz. Obrátí se proto na DNS server, který obsahuje rozsáhlou databázi IP adres na internetu, a ten mu ji sdělí, pokud ji DNS server nezná, zjistí si ji od dalšího DNS serveru na Internetu. Windows v příkazovém řádku pomocí příkazu nslookup a adresy serveru (například nslookup www.seznam.cz) zobrazí síťovou komunikaci, která nejprve vedla přes váš DNS server a posléze onen dotazovaný www server.



Obrázek 29: Zjištění IP adresy zadané domény

Zdroj: Vlastní zpracování

Pokud potřebujeme znát „vzdálenost" počítače (počet přechodů přes aktivní prvky a čas), lokalizaci v příslušné podsíti, resp. podsítě, přes které je komunikace realizována, lze použít příkaz ***tracert***.

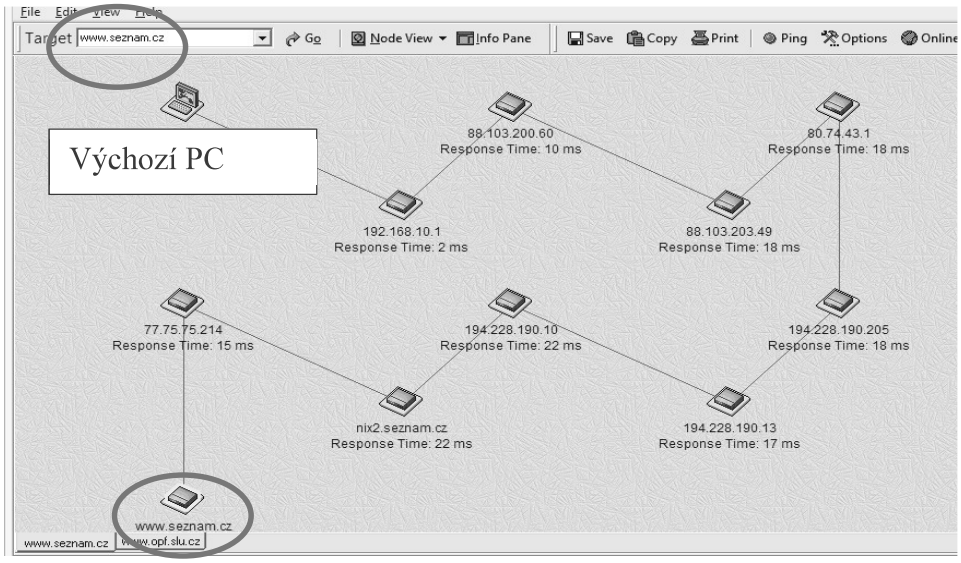


Obrázek 30: Příkaz tracert pro adresu www.seznam.cz

Zdroj: Vlastní zpracování

V praxi existuje nespočet aplikací, které využívají příkaz tracert ,dovedou „vytrasovat" cestu k cíli a zobrazit ji pomocí grafické nástavby. Následující obrázek ukazuje výpis programu NeoTrace Pro. Program dovede zobrazit cestu mezi počítači, časovou dostupnost i informace o síti ve které se příslušný aktivní síťový prvek nachází. Na následujícím obrázku

je výpis aktivních prvků při sledování dostupnosti serveru www.seznam.cz. Dále je ukázán výpis informací o počítači www.opf.slu.cz (z výpisu je zřejmé, že se jedná o server joanes.opf.slu.cz).



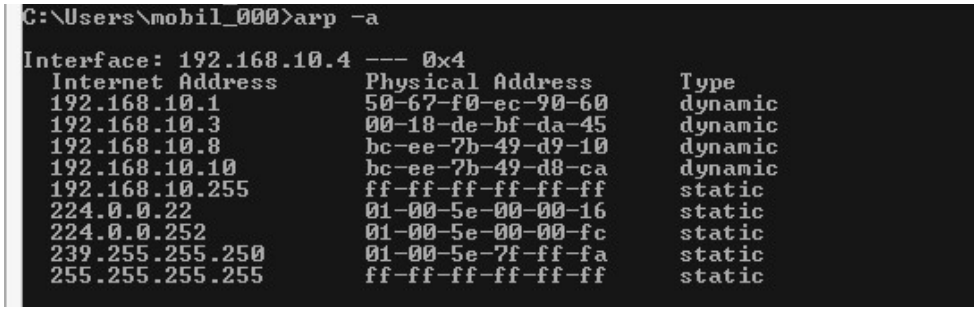
Obrázek 31: Trasování pomocí programu NeoTrace Pro

Zdroj: Vlastní zpracování

Obrázek 32: Informace o počítači z databáze RIPE

Zdroj: Vlastní zpracování

Údaje o dostupných okolních počítačích se ukládají v ARP tabulce. Zjištění evidovaných počítačů je možné příkazem ***arp - a*** pomocí protokolu arp (viz protokol TCP/IP), současně je evidováno, zda je adresa přidělená (dynamická) nebo pevně zadaná (statická).



Obrázek 33: Příkaz arp

Zdroj: Vlastní zpracování

3.3 Typy sítí dle jejich dosahu

Budeme-li se pohybovat v oblasti sítí, měli bychom zde zmínit alespoň okrajově základní členění sítí dle jejich dosahu. Některé z níže uvedených pojmů se již běžně nepoužívají, s jinými se však stále ještě setkáme:

3.3.1 WAN (Wide Area Network)

Tato zkratka reprezentuje počítačovou síť, která je z hlediska dosahu geograficky nejrozlehlejší. V obecné rovině je za WAN požadována síť Internet. Sítě WAN jsou používány pro propojení lokálních sítí nebo jiných sítí menšího rozsahu, tato zkratka je stále hojně používána. Budování takovýchto sítí je velmi nákladné a stalo se záležitostí těch největších hráčů na trhu. Můžeme se zde setkat s technologiemi jako ATM, X.25, MobileFI apod.

3.3.2 MAN (Metropolitan Area Network)

Označení, které bylo hojně používáno v USA v počátcích vznikající sítě internet. Jak vyplývá z jeho názvu, jednalo se o sítě geograficky příslušné svým rozsahem městu (často velkým městům). V Evropě se toto označení neuchytilo, snad z důvodu rychlého růstu dílčích sítí přesahujícího hranice měst.

3.3.3 LAN (Local Area Network)

Stále hojně používané označení pro lokální síť. Často se jedná o síť pokrývající svým rozsahem domácnost či firmu. Přenosové rychlosti v rámci těchto sítí bývají relativně vysoké, v současnosti nejrozšířenějšími technologiemi v LAN sítích jsou Ethernet či Wi-Fi.

3.3.4 PAN (PERSONAL AREA NETWORK)

V současné době často používaný pojem. Jedná se o malou „personální“ síť, tvořenou komunikujícími zařízeními, jako jsou např. mobilní telefony, PDA zařízení, či notebooky. Jedná se o malou síť, jejíž dosah bývá pouze několik metrů. Používá se pouze pro komunikaci samotných zařízení, popř. pro připojení do okolních sítí či k internetu. Rychlost připojení v rámci těchto sítí bývá pomalejší. Na této úrovni se můžeme setkat s technologiemi jako FireWire, USB, BlueTooth, IrDA apod.

3.4 Nejčastější síťové architektury v prostředí internetu

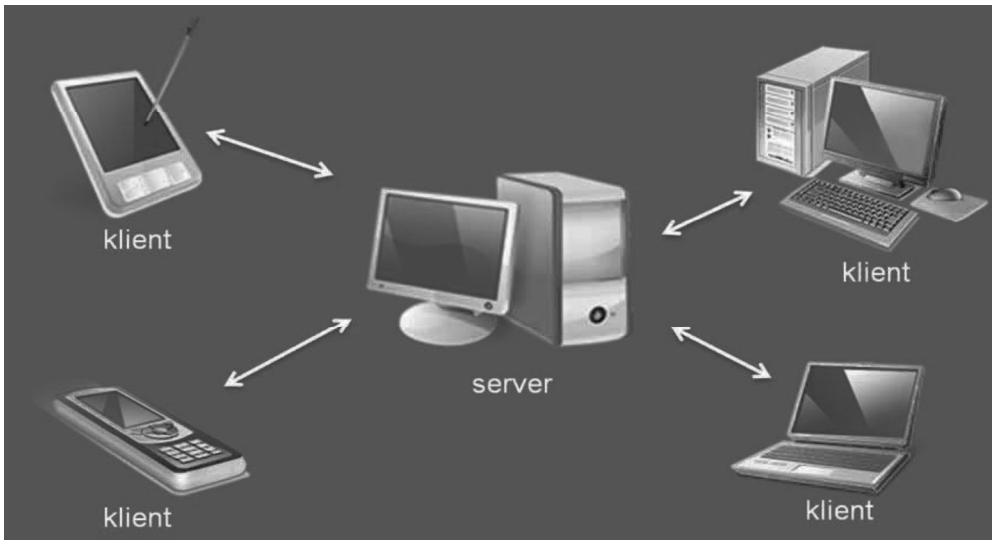
Budeme-li dále hovořit o internetových aplikacích, či o komunikaci mezi počítači v rámci internetu, je nutná alespoň základní představa o nejčastěji používaných síťových modelech v tomto prostředí.

3.4.1 ARCHITEKTURA KLIENT/SERVER

Architektura klient/server je jedním z nejčastěji používaných modelů v prostředí internetu.

Tento model, můžeme nalézt jak na hardwarové (fyzické propojení), tak na softwarové (komunikační) úrovni. Za server je v tomto případě považován počítač či aplikace poskytující určité služby ostatním. Jako příklad můžeme uvést tiskové servery, souborové servery či webové servery). V pozici klienta pak vystupují ostatní zařízení či klientské aplikace, které využívají služeb poskytovaných serverem. Z logiky věci je samozřejmě klientů větší počet.

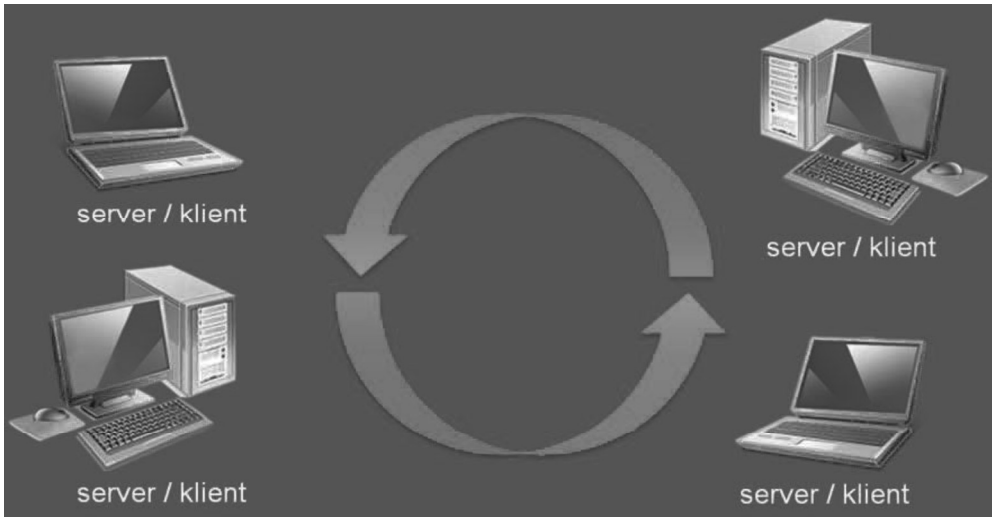
Oproti tomu architektura peer to peer (P2P), se vyznačuje tím, že všichni účastníci sítě vystupují jako server (poskytovatel služby či dat), a zároveň jako klient (využívají služeb). Tento model v poslední době nachází velké uplatnění v oblasti sdílení obsahu, např. v sociálních sítích.



Obrázek 34: Architektura klient/server

Zdroj: Botlík, Slaninová, 2014, Služby Internetu a internetové systémy, výukový materiál OPF v Karviné

3.4.2 ARCHITEKTURA P2P



Obrázek 35: Architektura P2P

SHRNUTÍ KAPITOLY

Kapitola měla představit pracovní nástroje pro práci se sítí, zejména pro identifikaci problémů souvisejících s dostupností počítačů v síti Internet. Byly představeny principy práce v počítačové síti, na konkrétních příkladech byly ukázány standardní nástroje a práce s TCP/IP protokolem. Byly ukázány základní síťové architektury.

4 ZÁKLADY INTERNETOVÝCH TECHNOLOGIÍ, SLUŽBY INTERNETU

RYCHLÝ NÁHLED KAPITOLY

V této kapitole se studenti seznámí se základními službami Internetu, provozovanými pomocí aplikačních protokolů TCP/IP protokolu. S tímto protokolem se seznámí důkladněji, včetně jeho srovnání s ISO/OSI modelem.

CÍLE KAPITOLY

Cílem kapitoly je seznámit studenty se základními pojmy, se kterými se setkají v kontextu fungování Internetu. Studenti po prostudování textu budou mít ujasněny vztahy mezi IP adresami a doménovými jmény a jejich přidělováním a správou. Na pojem internet se můžeme dívat z několika pohledů. Budeme-li se dívat na internet jako na medium, můžeme jej považovat za soubor technických prostředků umožňující šíření a sdílení dat (informací) v elektronické podobě po celém světě, a to bez omezení týkajících se typu a obsahu.

Na internet můžeme nahlížet také jako na celosvětovou počítačovou informační síť, která vznikla propojením samostatných dílčích sítí, ať už státních, univerzitních, regionálních či na federální úrovni (ve Spojených státech).

Federal Networking Council v roce 1995 definoval pojem internet jako globální informační systém, který:

- Je logicky propojen prostřednictvím globálně unikátního adresového prostoru založeného na protokolu IP, popř. na jeho rozšířeních a následnících,
- Je schopen zajistit vzájemnou komunikaci na základě rodiny protokolů TCP/IP, popř. na jeho rozšířeních a následnících (nebo pomocí protokolů kompatibilních s protokolem IP),
- Zajišťuje, používá a zpřístupňuje (veřejně či soukromě) služby vyšší úrovně na výše uvedené infrastruktuře.

Pojem internet se v odborné literatuře vyskytuje jako technický pojem (psáno s malým počátečním písmenem), pak jej chápeme jako technologicky propojenou počítačovou síť, která funguje na bázi protokolů (např. TCP, IP, UDP). V této rovině jsme se pak v dřívějších dobách ještě mohli setkat s dalšími pojmy, jako jsou intranet (vnitřní, interní síť organizace) či extranet (síť geograficky přesahující rozsah internetu).

Setkáme-li se s pojmem Internet (psáno s velkým počátečním písmenem), chápeme tento pojem jako název mezinárodní sítě (International Network), jako vlastní jméno celosvětové informační a komunikační sítě. Velmi často jsou laickou veřejností zaměňovány pojmy internet a WWW. Internet bychom měli chápat jako komunikační prostor pro výměnu, získávání a publikování informací, bez ohledu na jejich původ, formu, či jazyk. Kdežto WWW (World Wide Web) je zkratka služby poskytované samotným internetem. Jedná se o množinu propojených dokumentů a dalších zdrojů pomocí sítě odkazů.

ČAS POTŘEBNÝ KE STUDIU

Čas potřebný ke studiu v rozsahu 3-4 hodin, podle míry praktické práce.

KLÍČOVÁ SLOVA KAPITOLY

DNS, doména, IANA, NIC, infrastruktura, Cesnet, služby Internetu

4.1 Služby Internetu

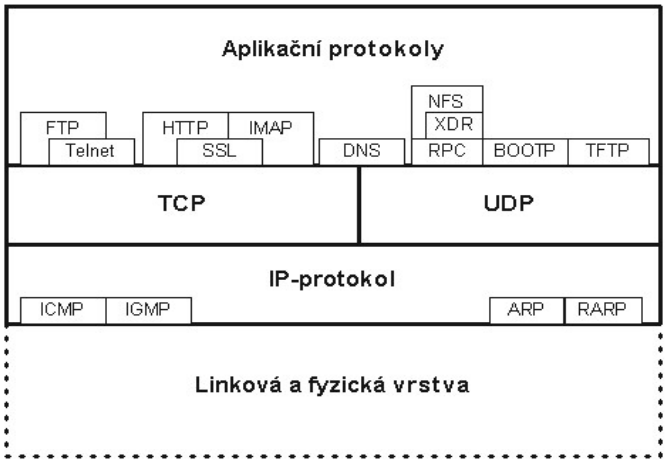
Pod pojmem „služby Internetu“ si většina laické veřejnosti představí chatování, stahování filmů a písniček nebo komunikaci a sdílení dat v sociálních sítích, popřípadě internetovou telefonii. V některých případech taky nákupy přes Internet elektronické bankovnictví či podobné služby. Tento výukový materiál se zabývá Internetovými službami založenými na aplikačních protokolech TCP/IP modelu, především službami pro přenos souborů, přenos hypertextů, správou elektronické pošty a vzdálenou správou. Je nutné si předem uvědomit, že vzhledem k povaze Internetu, který je v podstatě velkou počítačovou sítí, je nutné pro pochopení těchto služeb a jejich správu znát i elementární základy práce v počítačové síti.

4.2 Protokol TCP/IP

Vznik sady protokolů TCP/IP datujeme do sedmdesátých let 20. století[13]. Počátkem osmdesátých let byl protokol akceptován ministerstvem obrany USA jako perspektivní, v roce 1982: ministerstvo obrany USA přikazuje použití protokolů TCP/IP u všech sítí nově připojovaných k síti internet a od roku 1983 na protokoly TCP/IP přechází celý Internet.

[13] Text a obrázky převzato a částečně upraveno z Kabelová, Dostálek, 2010

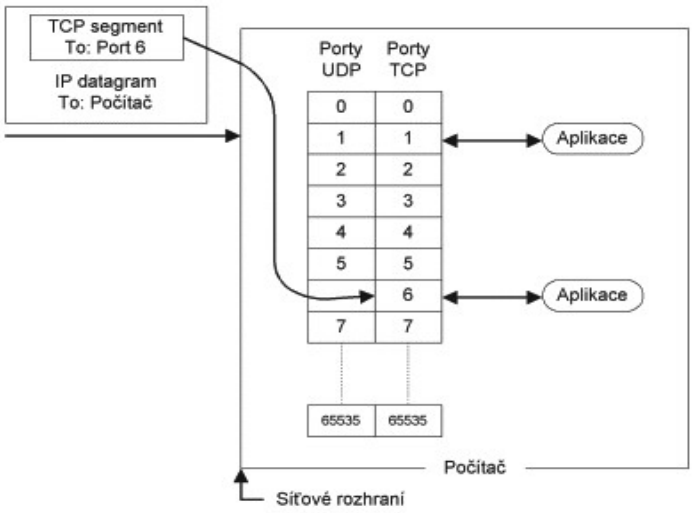
Rodina protokolů TCP/IP se nezabývá (až na výjimky) fyzickou a linkovou vrstvou. V praxi se i v Internetu používají pro fyzickou a linkovou vrstvu často protokoly vyhovující normám ISO OSI, které standardizoval ITU.



Obrázek 36: Protokoly a vrstvy TCP/IP modelu

Zdroj:Kabelová, Dostálek, 2010

Cílová aplikace je v Internetu adresována (jednoznačně určena) IP-adresou, číslem portu a použitým protokolem (TCP nebo UDP). Protokol IP dopraví IP-datagram na konkrétní počítač. Na tomto počítači běží jednotlivé aplikace. Podle čísla cílového portu operační systém pozná, které aplikaci má TCP-segment doručit.



Obrázek 37: TCP/IP adresace

Zdroj:Kabelová, Dostálek, 2010

4.2.1 TCP A UDP PROTOKOLY

Protokoly TCP a UDP odpovídají transportní vrstvě. TCP (resp. UDP) dopravuje data pomocí TCP segmentů (resp. UDP datagramů), které jsou adresovány jednotlivým aplikacím. Jinak řečeno, protokol TCP (resp. UDP) zajišťuje spojení mezi aplikacemi běžícími na vzdálených počítačích. Adresace je realizována prostřednictvím portů. Port si lze představit jako přechodový bod na rozhraní mezi transportní a aplikační vrstvou, který je jednoznačně identifikovatelný (svým číslem, tedy tzv. číslem portu). Samotný port však není ani odesilatelem, ani příjemcem – tím je entita aplikační vrstvy (například systémový proces, aplikace úloha apod.), která se "přidruží" k příslušnému portu a skrz něj komunikuje s entitami transportní vrstvy (které implementují protokoly TCP či UDP). Protokol TCP je spojovanou službou (connection oriented), tj. službu která mezi dvěma aplikacemi naváže spojení – vytvoří na dobu spojení virtuální okruh. Tento okruh je plně duplexní (data se přenášejí současně na sobě nezávisle oběma směry). Přenášená data jsou číslována. Ztracená nebo poškozená data jsou znovu vyžádána. Konce spojení (“odesilatel” a “adresát”) jsou určeny číslem portu z rozsahu hodnot 0 až 65535. U čísel portů se rozlišuje, zde se jedná o porty protokolu TCP nebo UDP (za číslo napíše lomítko a TCP nebo UDP, port 53/tcp nemá nic společného s portem 53/udp). Základní jednotkou přenosu v protokolu TCP je TCP segment. TCP segment se vkládá do IP-datagramu. IP-datagram se vkládá do linkového rámce. Protokol UDP je jednoduchou alternativou k protokolu TCP. Protokol UDP je nespojovaná služba (na rozdíl od protokolu TCP), tj. nenavazuje spojení. Odesilatel odešle UDP datagram příjemci a nepožaduje potvrzení o přijetí. UDP datagramy jsou baleny do IP-datagramu.

Číslo	TCP	UDP	Služba
20	tcp	udp	FTP (data)
21	tcp	udp	FTP (příkazy)
22	tcp	udp	SSH
23	tcp	udp	Telnet
25	tcp	udp	SMTP
53	tcp	udp	DNS
66	tcp	udp	Oracle SQL*NET
80	tcp	udp	HTTP
88	tcp	udp	Kerberos
110	tcp	udp	Post Office Protocol - Version 3, POP3
143	tcp	udp	IMAP
366	tcp	udp	SMTP, Simple Mail Transfer Protocol
443	tcp	udp	HTTPS
647	tcp		DHCP Failover Protocol
993	tcp		IMAPS, SSL
995	tcp		POP3S, SSL
5800	tcp		VNC - Java klient
5900	tcp		VNC

Tabulka 1 Přehled nejčastějších portů

Adresátem UDP datagramu nemusí být pouze jednoznačná IP-adresa, tj. síťové rozhraní konkrétního počítače. Adresátem může být skupina stanice – adresovat lze tzv. oběžník. Adresovat lze všeobecné oběžníky (broadcast), nebo adresné oběžníky (multicast).

4.2.2 IP PROTOKOL

IP protokol přenáší tzv. IP-datagramy mezi vzdálenými počítači. Každý IP-datagram ve svém záhlaví nese adresu příjemce, což je úplná směrovací informace pro dopravu IP-datagramu k adresátovi. Adresace je realizována pomocí IP adresy. Síť může přenášet každý IP-datagram samostatně. IP-datagramy tak mohou k adresátovi dorazit v jiném pořadí, než byly odeslány. Každé síťové rozhraní v síti Internet má svou celosvětově jednoznačnou IP-adresu (jedno síťové rozhraní může mít více IP-adres, avšak jednu IP-adresa nesmí používat více síťových rozhraní).

Některé linkové protokoly jsou určeny pro dopravu dat v rámci lokální sítě, jiné linkové protokoly dopravují data mezi sousedními směrovači rozsáhlé sítě. IP-protokol na rozdíl od linkových protokolů dopravuje data mezi dvěma libovolnými počítači v Internetu, tj. přes více LAN.

Data jsou od odesilatele k příjemci dopravována (směrována) přes směrovače (router). Na cestě od odesilatele k příjemci se může vyskytnout cela řada směrovačů. Každý směrovač řeší samostatně směrování k následujícímu směrovači. Data jsou tak předávána od směrovače k směrovači. Z angličtiny se ustálil výraz následující hop (next hop), jako následující uzel, kam se data předávají. Hopem se rozumí buď následující směrovač, nebo cílový stroj.

IP-protokol je tvořen vlastním protokolem IP a několika dílčími protokoly.

Protokol ICMP je služební protokol, který je součástí IP-protokolu. Protokol ICMP slouží k signalizaci mimořádných událostí v sítích postavených na IP-protokolu. Protokol ICMP svoje datové pakety balí do IP-protokolu, tj. pokud budeme prohlížet přenášené datagramy, pak v nich najdeme za linkovým záhlavím záhlaví IP-protokolu následováno záhlavím ICMP paketu. Základními funkcemi a indikovanými hodnotami jsou echo, nedoručitelný datagram, volba rychlosti odesílání, žádost o směrování změna směrování, maska podsítě, synchronizace dat, vypršení doby životnosti apod.

Protokol IGMP je podobně jako protokol ICMP služebním protokolem (podmnožinou) protokolu IP. Pakety IGMP-protokolu jsou baleny do IP-datagramů. Protokol IGMP slouží k šíření adresných oběžníků (multicasts)

Protokol ARP (Address Resolution Protocol) řeší problém zjištění linkové adresy protější stanice ze znalosti její IP-adresy vysláním linkového oběžníku (linková adresa

FF:FF:FF:FF:FF:FF) s prosbou: "Já stanice o linkové adrese HW1, IP-adrese IP1, chci komunikovat se stanicí o IP-adrese IP2, kdo mi pomůže s na nalezením linkové adresy stanice o IP-adrese IP2? Stanice IP2 takovou žádost uslyší a odpoví. V odpovědi uvede svou linkovou adresu HW2.

Protokol ARP určuje jednoznačný vztah mezi jednoznačnou IP-adresou příjemce (unicast) a linkovou adresou příjemce. To je možné tehdy, když mezi IP-adresami a linkovými adresami existuje jednoznačný vztah. Tento vztah se anglicky nazývá mapping, tj. mapování IP adres na linkové adresy.

4.2.3 APLIKAČNÍ PROTOKOLY

Aplikační protokoly v TCP/IP modelu odpovídají několika vrstvám ISO OSI. (Relační, prezentační a aplikační vrstva).

Prostřednictvím aplikačních protokolů se zabezpečují služby aplikací. Nečastěji používané protokoly jsou patrné z obr. 27. Mezi nejpoužívanější protokoly patří telnet (i když z důvodu bezpečnosti je na ústupu), FTP, HTTP, POP3, IMAP, SMTP, DNS, DHCP, SSH a další.

Telnet

Protokol Telnet slouží pro tzv. vzdálené přihlašování, neboli k tomu, aby uživatel jednoho počítače získal přístup ke vzdálenému počítači prostřednictvím vzdáleného terminálu. Na displeji lokálního počítače je zobrazen displej vzdáleného počítače, klávesnice se chová jako připojená ke vzdálenému počítači. V dnešní době existuje poměrně velká skupina kvalitnějších aplikací jako VNC, TeamViewer apod. Přesto má telnet své místo, především pro vzdálenou správu na úrovni příkazového řádku a využívání výpočetní kapacity vzdáleného počítače (aplikace, soubory, periferie apod.). Protokol Telnet je koncipován tak, aby umožňoval "spolupráci" různých platforem – není závislý na prostředí klientského počítače (ze které se uživatel přihlašuje ke vzdálenému počítači) ani serveru (vzdálený počítač). Díky tomu je například možné, aby se prostřednictvím protokolu Telnet uživatel počítače PC s MS Windows přihlásit na dálku k Unixovému počítači, a pracoval s Unixovými aplikacemi, které běží na tomto vzdáleném počítači a na jeho počítači PC by provozovány být nemohly.

HTTP

(HyperText Transfer Protocol) slouží k přenosu hypertextových souborů vytvořených jazykem HTML. Na vzdáleném počítači musí být spuštěn HTTP server a na lokálním HTTP klient (prohlížeč HTML, např. Internet Explorer). HTTP má vyhrazen TCP port 80. Protokol umožňuje prohlížeči vyžádat si na serveru konkrétní WWW stránku, a následně ji zobrazit na klientském počítači. Tento protokol je spolu s elektronickou poštou nejvíce používaným a zasloužil se o obrovský rozmach internetu v posledních letech. Samotný protokol HTTP neumožňuje šifrování ani zabezpečení integrity dat. Pro zabezpečení HTTP se často používá TLS spojení nad TCP. Toto použití je označováno jako HTTPS (Security

Hyper Text Transfer Protocol) slouží k přenosu zašifrovaných hypertextových souborů typu HTML. Na vzdáleném počítači přitom musí být spuštěn HTTP server s podporou šifrování (tzv. SSL protokolem).

FTP

(File Transfer Protocol) je protokol pro přenos souborů mezi uzlovými počítači sítě, může být používán nezávisle na použitém operačním systému.

SMTP

(Simple Mail Transfer Protocol) je používán pro přenos (odesílání) elektronické pošty. SMTP server má vyhrazen port 25. Klient s ním komunikuje prostřednictvím klientské aplikace, nebo zasíláním příkazů z příkazového řádku (například příkazy služby telnet).

POP3

(Post Office Protocol, v současnosti verze 3) zajišťuje komunikaci mezi poštovním serverem a osobním počítačem uživatele, je určen ke stahování došlé pošty z poštovního serveru. Služba běží na TCP portu 110. Klient s ním komunikuje prostřednictvím klientské aplikace, nebo zasíláním příkazů

IMAP

(Internet Message Access Protocol) je 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. V současné době se používá protokol IMAP4.

4.3 Služby založené na aplikačních protokolech

Komunikace v prostředí sítí a od toho se odvíjející služby mohou být v podstatě dvojího typu. V případě, že každý počítač (uživatel, aplikace) definuje, které prostředky a v jakém rozsahu poskytne ostatním a následně komunikaci neřídí, ale ponechává na přistupujícím počítač, jedná se o síť „rovný s rovným“ označovanou jako peer to peer. V této síti není „řídící“ počítač, každý má stejná práva a schopnosti, které si sám určuje.

Základní služby Internetu jsou založeny na architektuře (principech, formě komunikace), kdy jeden počítač poskytuje prostředky a služby (server) a ostatní počítače k těmto službám přistupují (klienti). Tato architektura je označována jako server/klient (klient/server). Jako server si můžeme představit hardwarový prostředek, na kterém se příslušná

služba provozuje (počítače označené jako servery, dislokované zpravidla v tzv. „serverovnách“. Prakticky je ale server zabezpečován aplikací, která na příslušném počítači běží (serverem tedy může být libovolný počítač, na kterém je spuštěna příslušná aplikace).

Serverová aplikace zabezpečuje práva uživatelů (klientů), disponibilní prostředky, pravidla, formy komunikace a správu dat. Data jsou umístěna centrálně na datovém prostředku (disk, datové pole) obsluhovaném serverem. Pro přístup k datům a jejich organizaci mohou být využívány další softwarové produkty (databáze, programy apod.).

Klient (uživatel, počítač, aplikace) prostřednictvím specifického software přistupuje k aplikacím zabezpečovaným serverem.

(Ve firemním prostředí může být typickým příkladem software pro účetnictví. Software je nainstalovaný na jednom počítači, na kterém jsou současně uložena data. K programu přistupují klienti (účetní) z jiných PC prostřednictvím klientské části účetního software, mají nadefinované role a práva a přidělenou část prostředků, které mohou spravovat, např. faktury., sklad apod.). Blíže byly tato principy popsány v kapitole 1.6.

4.3.1 FTP

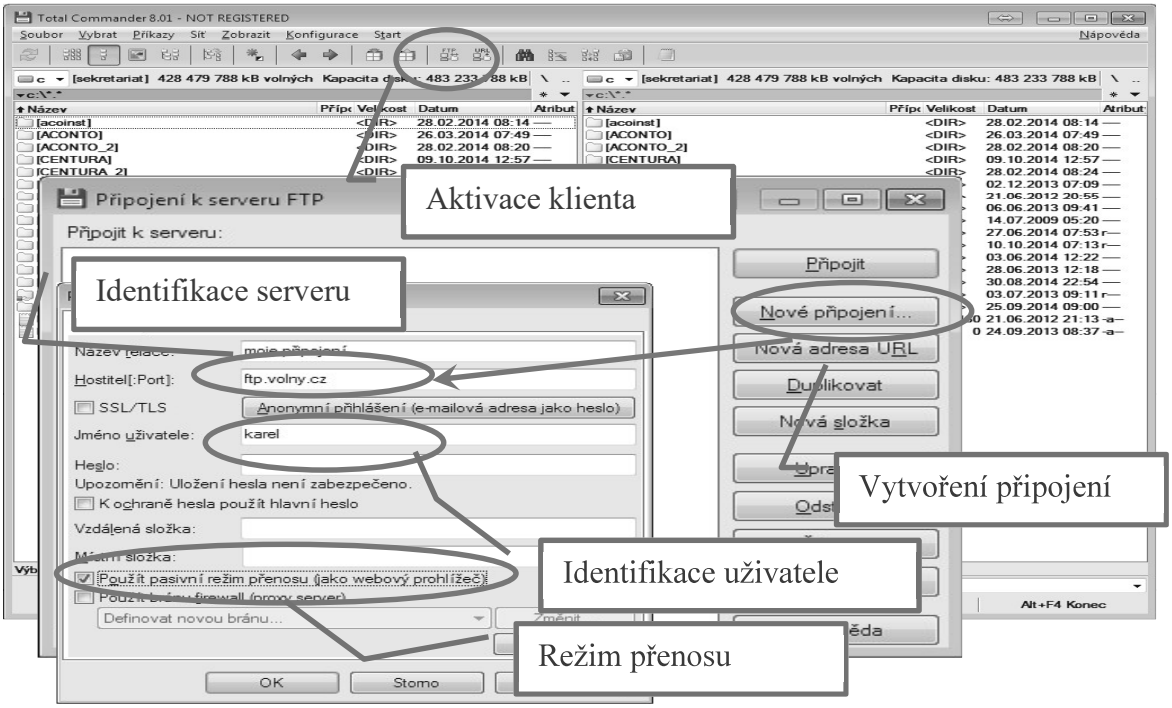
FTP je jeden z nejstarších protokolů, využívá porty TCP/21 a TCP/20. Pakety na portu 21 slouží k řízení komunikace – řídicí kanál. Port 20 slouží k vlastnímu přenosu dat – datový kanál. Porty klienta jsou dynamické a přiděluje je OS. Protokol je interaktivní a umožňuje řízení přístupu (přihlašování login/heslo), specifikaci formátu přenášeného souboru (znakově – binárně), výpis vzdáleného adresáře atd. V současné době není považován za bezpečný a z tohoto důvodu pro něj byla definována některá rozšíření (RFC 2228). Hesla a soubory jsou ve standardním protokolu zasílána jako běžný text (nejsou šifrovaná) což silně snižuje bezpečnost (ohrožuje jméno, heslo, ale i přenášená data). Protokol FTP stanoví pravidla komunikace mezi klientem a serverem. Jedná se o spojovanou spolupráci. Klient naváže spojení se serverem, předá uživatelské jméno a heslo. Po navázání spojení může probíhat práce s adresáři a soubory a přenos dat mezi klientem a serverem. Spojení se obvykle ukončí z podnětu klienta. Úsek komunikace mezi otevřením a uzavřením spojení se nazývá relace. Řídicí kanál se po dobu relace otevře jen jednou a zůstává otevřen, zatímco datový se po přenosu dat (souboru) uzavře a pro každý datový přenos je nutné kanál znovu otevřít. Podle toho, kdo otevírá datový kanál, se rozlišuje aktivní a pasivní režim spojení. Přenos souborů probíhá v textovém nebo binárním režimu v závislosti na typu souboru nebo potřebách uživatele. Chování serveru nebo klientského programu je určeno konfigurací. O komunikaci lze vést na obou stranách spojení protokol. Aplikační protokol FTP využívá vrstvy TCP k zabezpečenému přenosu datových segmentů. Prostřednictvím klientského programu telnet lze zabezpečit přenos datových segmentů, i když komunikujeme se serverem na jiném portu než 23, tj. např. na portu 21; příkazy pak musejí být přímo příkazy protokolu FTP. V protokolu je použit model klient-server. FTP server poskytuje data pro ostatní počítače. Klient se k serveru připojí a může provádět různé operace (výpis adresáře, změna adresáře, přenos dat atd.). Operace jsou řízeny sadou příkazů, které

jsou definovány v rámci FTP protokolu, proto kdokoliv může vytvořit klienta pro jakékoliv prostředí nebo operační systém. Existuje mnoho programů pro FTP servery i klienty a mnoho je jich volně dostupných. Operační systém MS Windows má implementovaného klienta FTP, spustitelného pomocí příkazové řádky. Seznam dostupných příkazů je k dispozici příkazem ***help***.

Obrázek 38: Příkazy FTP dostupné v příkazovém řádku

Zdroj::vlastní zpracování

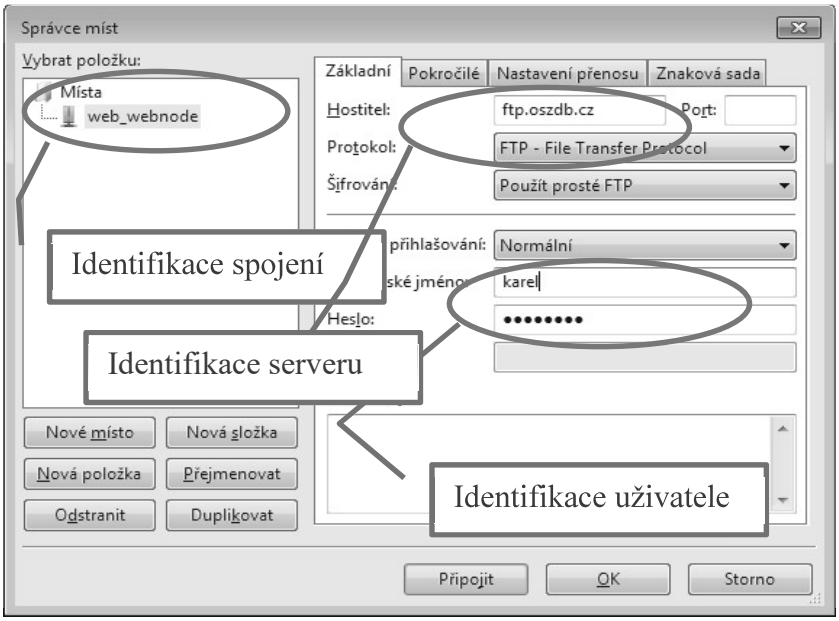
Mezi nejrozšířenější FTP klienty patří Windows Commander (Total Commander). Program umožňuje nadefinovat připojení a ve dvou oddělených oknech zobrazovat soubory lokálního a vzdáleného počítače, jako by se jednalo o soubory lokální.



Obrázek 39: Total Commander jako FTP klient

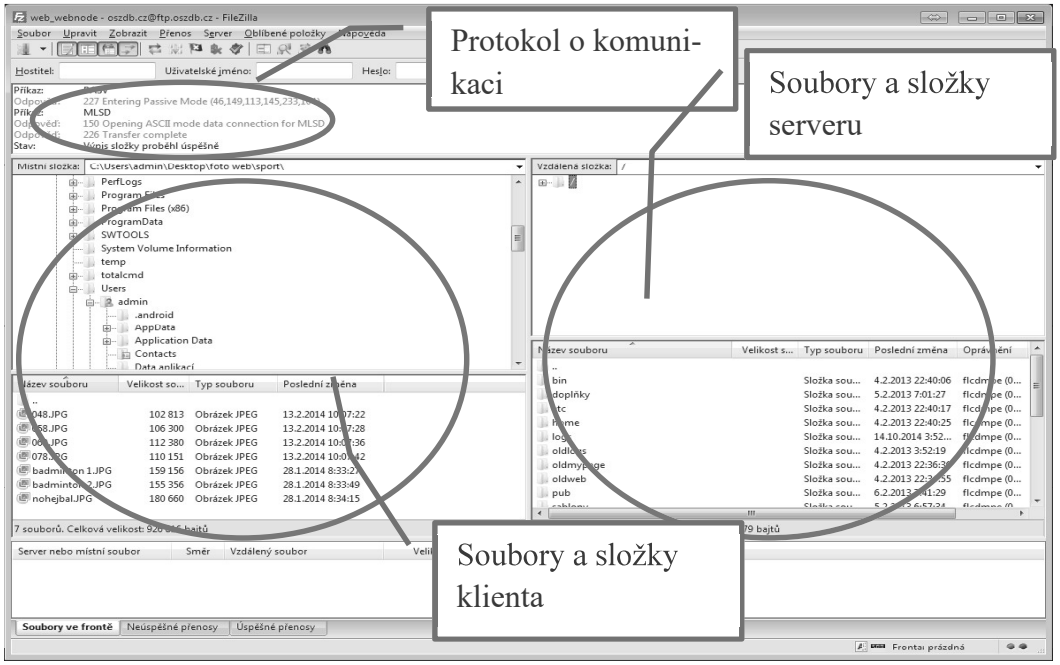
Zdroj::vlastní zpracování

Dalším, poměrně výkonným klientem je software FileZilla, který je k dispozici rovněž jako serverová aplikace. Software umožňuje definování množiny připojení, správu souborů včetně práce s atributy apod. Základní nastavení spojení a správu souborů ukazují následující obrázky.



Obrázek 40: FTP klient FileZilla

Zdroj::vlastní zpracování



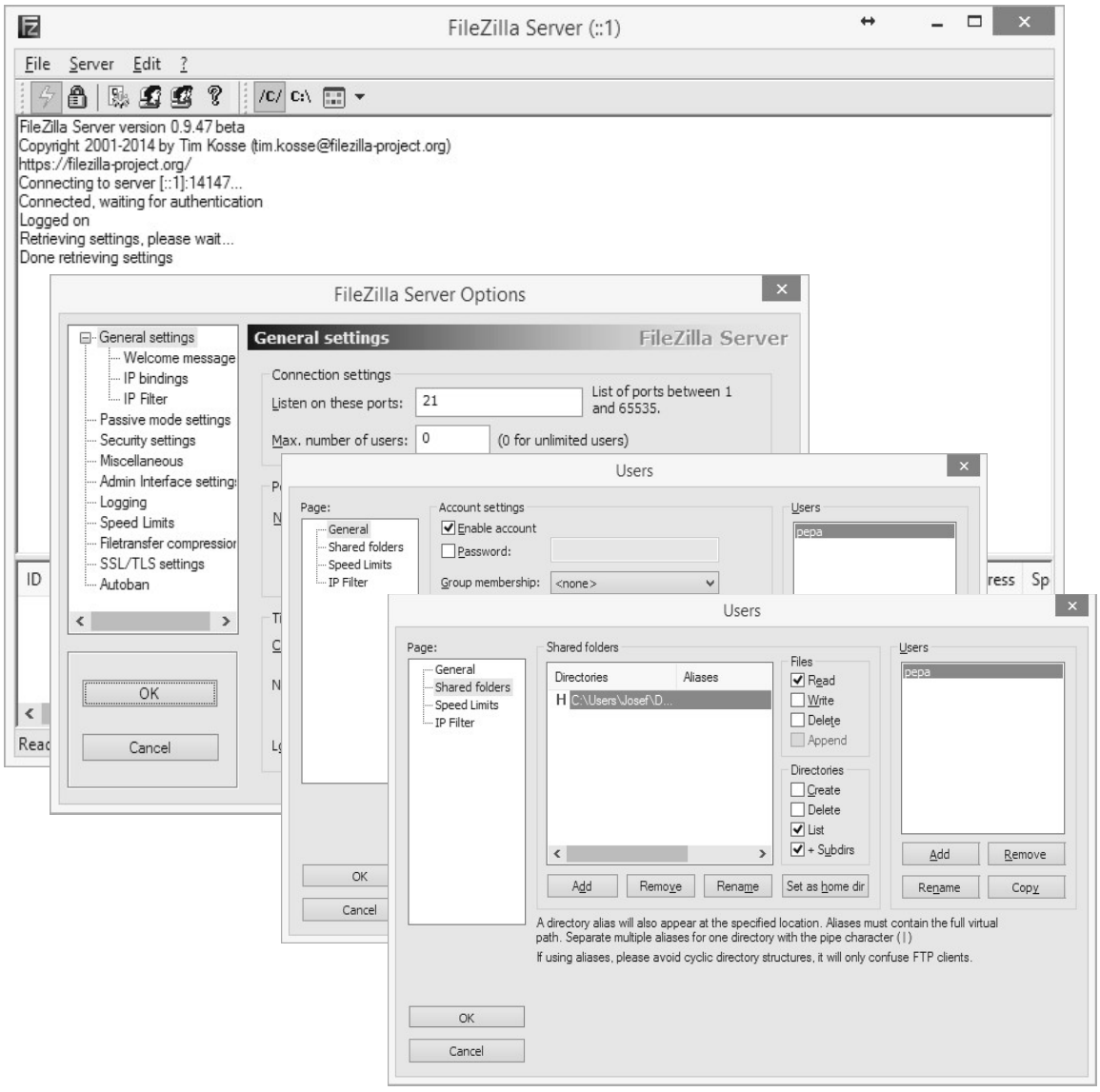
Obrázek 41: Pracovní oblast FileZilla klienta

Zdroj::vlastní zpracování

Jako klient FTP v dnešní době funguje i většina www prohlížečů.

Pokud chceme aktivně využívat FTP službu a provozovat vlastní FTP server musíme mít příslušný software. V segmentu Free aplikací je velmi výkonnou serverovou aplikací např. Caesar nebo FileZilla server.

ákladní nastavení FTP serveru spočívá ve vytvoření skupin uživatelů, nastavení pracovních prostorů, uživatelských jmen a hesel a uživatelských práv. K serveru můžeme v lokální síti přistupovat prostřednictvím IP adresy počítače, na kterém je příslušný software provozován.



Obrázek 42: Základní nastavení serveru FileZilla

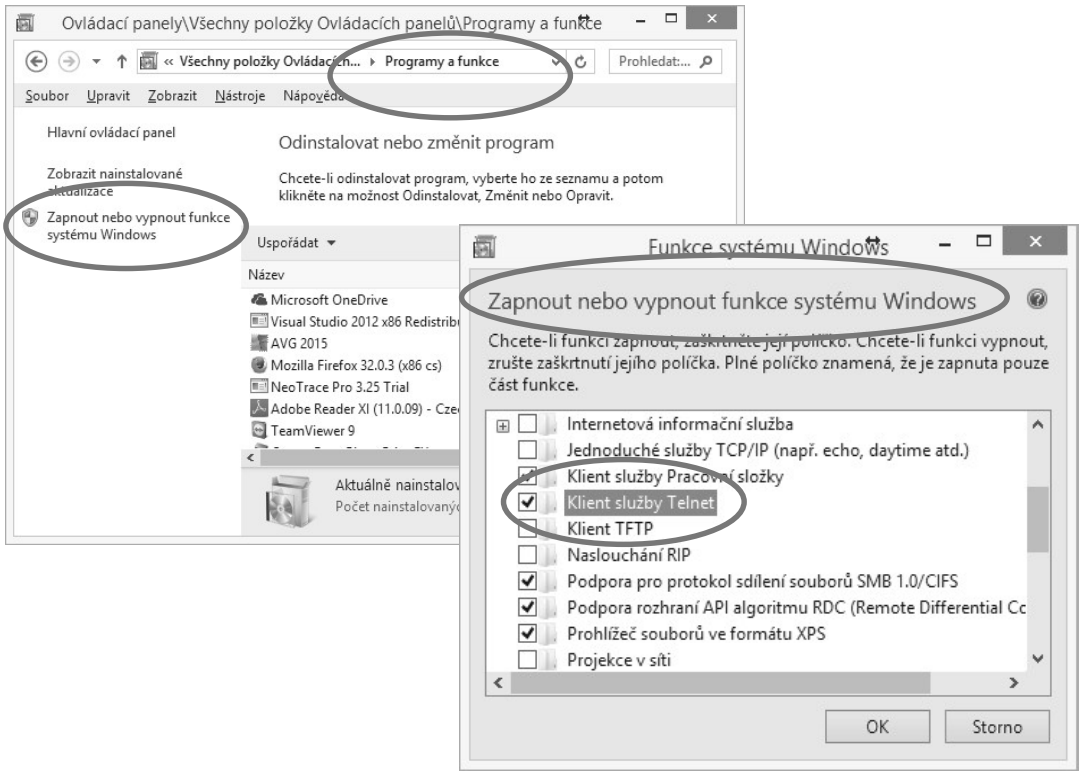
Zdroj:: vlastní zpracování

4.3.2 TELNET

Telnet je aplikační protokol TCP/IP, program, pro komunikaci mezi dvěma počítači pomocí telnet protokolu a služba pro vzdálený přístup. Program je dodnes součástí Microsoft Windows a unixových systémů. Dříve se používal (spolu s protokolem telnet) pro připojení ke vzdálenému počítači prostřednictvím počítačové sítě jako emulace terminálu, která poskytovala možnost práce uživatele na vzdáleném počítači v příkazovém řádku. Telnet tak byl nástupcem terminálů, ze kterých se uživatelé připojovali ke vzdálenému počítači pomocí sériové linky. Hlavní nevýhodou telnetu je absence šifrování přenášených dat, a proto dnes uživatelé místo telnetu používají protokol SSH. V současné době se program telnet používá pro komunikaci mezi počítačovými programy (například simulace připojení webového prohlížeče k webovému serveru, při simulaci SMTP protokolu pro přepravu elektronické pošty a podobně).

Standardně není u novějších verzí příkaz telnet k dispozici. Přesto je telnet klient i telnet server součástí instalace, není však z bezpečnostních důvodů aktivní.

Aktivaci klienta i serveru lze provést v nabídce ovládací panely – programy a funkce (přidat ubrat programy) – zapnout nebo vypnout funkce systému windows.



Obrázek 43: aktivace klienta telnet v MS Windows

Zdroj::vlastní zpracování

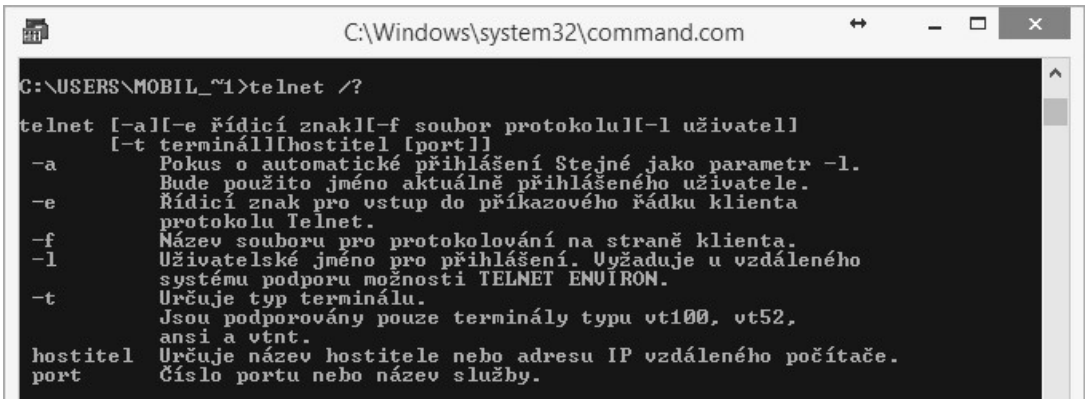
Po aktivaci lze klienta spustit jako příkaz v příkazové řádce. Parametrem „?“ lze opět vypsat možnosti příkazu a parametry příkazu.

Příkazy Telnet se mohou nepatrně lišit podle verze OS, respektive podle použitého klienta. Seznam příkazů pro klienta MS Windows je dostupný např. na http://windows.microsoft.com/cs-cz/windows/telnet-commands#1TC=windows-7.

Vytvořit připojení programu Telnet k hostitelskému počítači nebo vzdálenému serveru lze příkazem ***open*** nebo ***o.*** Standardně se pro komunikaci používá port 23, lze jej však změnit, chceme-li přistupovat ke službě zabezpečované jiným protokolem.

Příkaz ***open ftp.opf.slu.cz 100*** by otevřel komunikaci se serverem ftp.opf.slu.cz (pokud by existoval) na portu 100.

Ukončit existující připojení programu Telnet lze příkazem ***close*** (***c***). Může být použit v kombinaci s názvem hostitele a číslem portu.



Obrázek 44: atributy příkazu telnet

Zdroj::vlastní zpracování

Příkaz ***display*** zobrazí aktuální nastavení klienta služby Telnet (seznam aktuálních pracovních parametrů). Úpravu parametrů je nutné provádět mimo relaci.

Ukončit program Telnet lze příkazem ***quit*** (***q***). Příkaz ***set n***astaví typ terminálu pro připojení, zapne místní odezvu, nastaví ověřování NTLM, znak escape a protokolování, vypnutí místní odezvy nebo nastavení ověřování pro zadávání uživatelského jména a hesla při přihlašování lze provést příkazem ***unset***. Příkaz ***status*** zjistí, zda je klient služby Telnet připojen.

4.3.3 POŠTOVNÍ SLUŽBY

E-mailové zprávy jsou obecně posílány e-mailovému serveru, který ukládá příchozí zprávy v příjemcově mailboxu. Uživatel později znovu získává tyto zprávy buď přes we-

bový prohlížeč, nebo přes e-mailového klienta, který používá jeden z e-mailových protokolů. Zatímco někteří klienti a servery upřednostňují používání vlastních protokolů, zároveň podporují i standardní protokoly (SMTP pro odesílání, pro přijímání se používá POP3 a IMAP), což jim dovoluje komunikovat s ostatními klienty

Poštovní klient je program, který zajišťuje odesílání zpráv a vybírání schránek. Příkladem je např. Microsoft Outlook, Mozilla Thunderbird, Opera a další. Je to v podstatě specializovaný editor, který umí kromě vytvoření zprávy také manipulovat se schránkami, odeslat zprávu nejbližšímu serveru a převzít zprávu ze serveru prostřednictvím POP3 nebo IMAP. Vlastním doručováním zprávy po síti až k adresátovi se klient nezabývá. Součástí klienta bývá adresář, který pomáhá uživateli udržet přehled o adresách.

Poštovní server (MTA) běží obvykle jako démon či Služba Windows a naslouchá na portu TCP/25. K tomuto portu se může připojit (navázat TCP spojení) buď poštovní klient, nebo jiný server, který předá zprávu k doručení. MTA zkontroluje, zda je zpráva určena pro systém, na kterém běží. Pokud ano, předá ji programu MDA (lokální doručení). Pokud je zpráva určena jinému počítači, naváže spojení s příslušným serverem a zprávu mu předá.

Při vyhledávání vzdáleného serveru, kterému má předat zprávu, musí MTA spolupracovat se systémem DNS. Od serveru DNS si vyžádá záznam pro cílovou doménu, který obsahuje IP adresu počítače, který se stará o doručení pošty v této doméně. Pokud DNS tento záznam neobsahuje, pokusí se poštovní server doručit zprávu přímo na počítač uvedený v adrese za zavináčem.

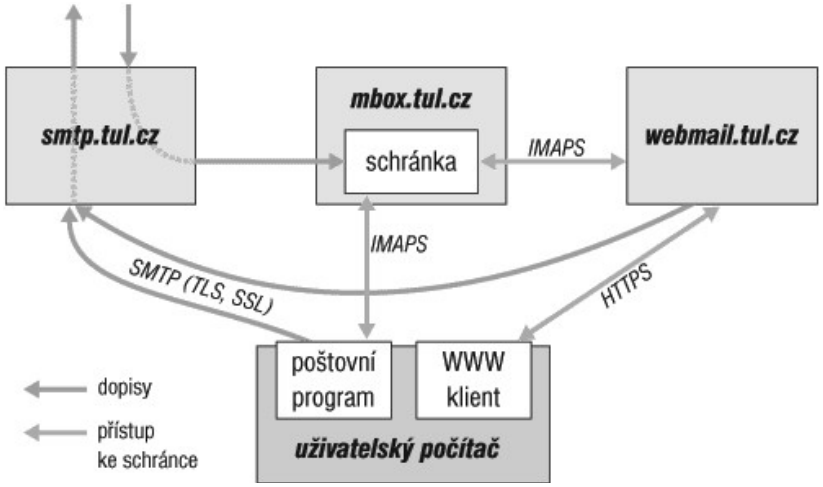
Poštovní server obsahuje v konfiguraci řadu parametrů, pomocí kterých můžeme mimo jiné nastavit, pro které domény MTA přijímá zprávy. Stejně tak je možné určit, od koho bude nebo nebude zprávy přijímat, což je velmi důležité z hlediska bezpečnosti a ochrany proti spamu.

Jako příklad fungování elektronické pošty a příslušných protokolů si ukážeme poštovní servery a komunikaci na technické univerzitě v Liberci[14].

Jádro systému elektronické pošty tvoří tři servery:

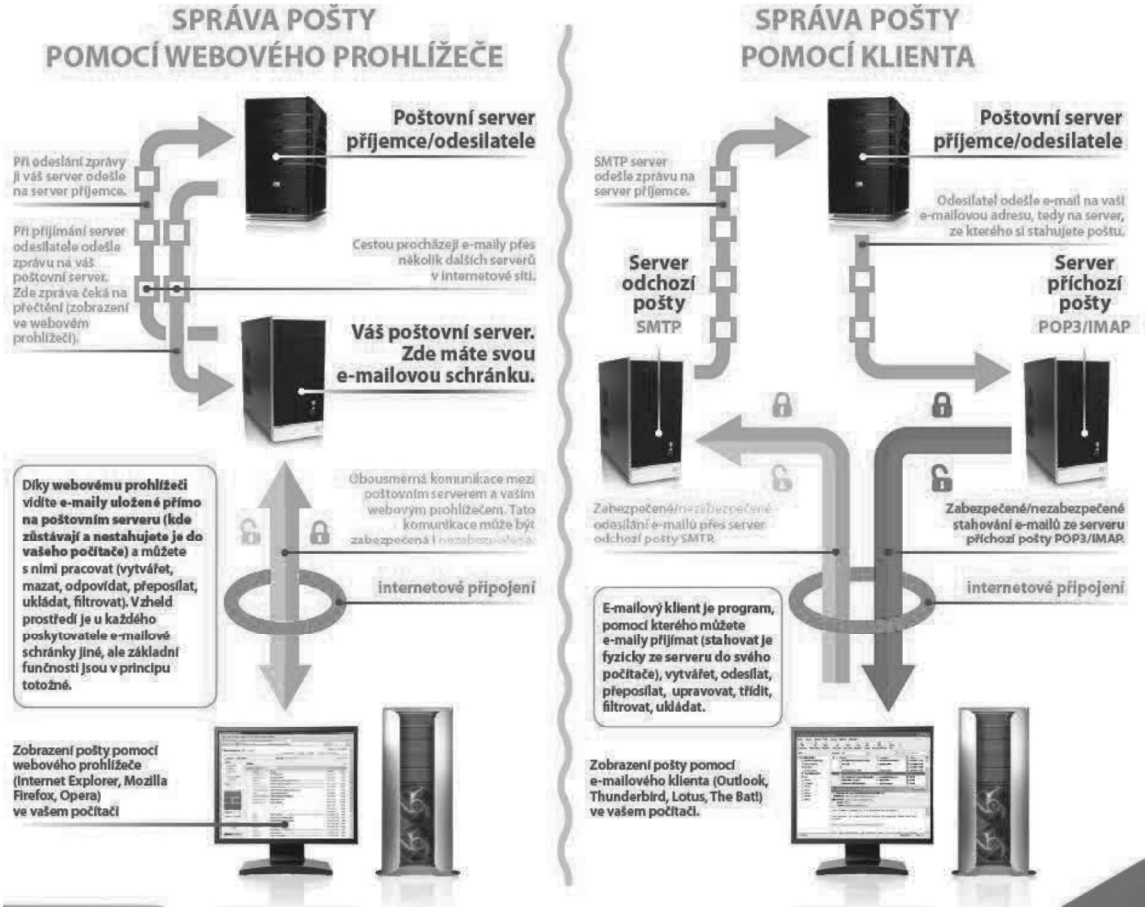
- mbox.tul.cz – zajišťuje příjem pošty a vede poštovní schránky uživatelů
- webmail.tul.cz – poskytuje přístup k elektronické poště prostřednictvím WWW rozhraní
- smtp.tul.cz – slouží k odesílání elektronických dopisů; jeho prostřednictvím také přichází elektronická pošta zvenčí

[14] Převzato [online]. [vid. 1.9 2013]. Dostupné z: http://liane.tul.cz/cz/Elektronick%C3%A1_po%C5%A1ta



Obrázek 45: poštovní servery a přístup k poště - příklad TUL

Zdroj: [online]. [vid. 1.9 2013]. Dostupné z:http://liane.tul.cz/cz/Elektronick%C3%A1_po%C5%A1ta



Obrázek 46: schéma správy pošty pomocí www klienta a poštovního klienta[15]

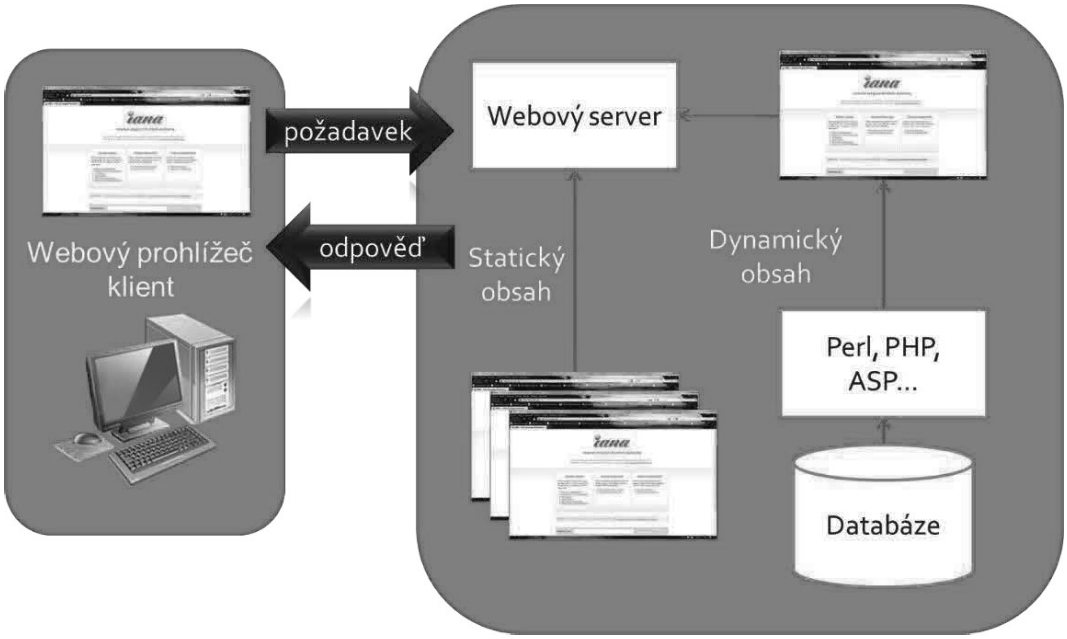
Zdroj: [online]. [vid. 1.9 2013]. Dostupné z:http://www.urazydeti.cz/kit/postery/d03.pdf

[15] Převzato [online]. [vid. 1.9 2013]. Dostupné z:http://www.urazydeti.cz/kit/postery/d03.pdf

4.3.4 HTTP

Prostřednictvím aplikačního protokolu http (HyperText Transport Protokol, někdy též HyperText Trasfer Protokol)) je zabezpečována služby www stránek, WWW stránky jsou dokumenty psané ořevážně v html (HyperText Markup Language). Používá obvykle port TCP/80. Protokol funguje způsobem dotaz-odpověď. Uživatel (pomocí programu, obvykle internetového prohlížeče) pošle serveru dotaz, obsahujícího označení požadovaného dokumentu, informace o prohlížeči apod. Server poté odpoví, zda se dokument podařilo najít, jakého typu dokument je atd., a zašle data samotného požadovaného dokumentu.

Při poskytování této služby je tedy využívána architektura klient/server, viz například Kapitola 3.4. Pod pojmem server si zde můžeme představit WWW server, který poskytuje informace v podobě WWW stránek, případně může poskytovat i další obsah. Pojem klient pak představuje prohlížeč (browser), který je nainstalovaný na zařízení uživatele (počítač, notebook, mobilní zařízení). Jeho úlohou je pak zobrazení webových stránek a případně přehrávání dalšího obsahu. Princip komunikace je znázorňuje obrázek.



Obrázek 47: Služba www - princip komunikace

Zdroj: Botlík, Slaninová, 2014, Služby Internetu a internetové systémy, výukový materiál OPF v Karviné

4.4 Organizace v prostředí internetu

I když se zdá být vývoj internetu a internetových technologií poněkud překotný, až chaotický, existují organizace, které se snaží svým způsobem tento vývoj usměrňovat. Následující text uvádí nejdůležitější z nich.

ISOC[16] (INTERNET SOCIETY)

Tato nezisková organizace, založená v roce 1992 působí jako zastřešující orgán všech dalších organizací působících v oblasti internetu. Hlavním cílem organizace je podpora otevřeného rozvoje a využívání Internetu po celém světě, snaží se o koordinaci skupin odpovědných za vývoj standardů (podrobněji viz dále).

IETF[17] (INTERNET ENGINEERING TASK FORCE)

IETF je vedoucí organizace v oblasti internetových standardů, která úzce spolupracuje s ISOC. Jedná se o sdružení odborníků z počítačového průmyslu, provozovatelů sítí a telekomunikací. Jejich hlavním cílem je rozvoj technických řešení, nových technologií, jejich výběr a příprava pro schvalování. Působnost této organizace je velmi široká, zasahuje do různých tematických oblastí, jako aplikace, protokol IP, Internet, správa sítí, bezpečnost apod.

IAB[18] (INTERNET ARCHITECTURE BOARD)

IAB je organizace zabývající se otázkami celkové architektury internetu. Drží dozor nad organizací IETF. Má poradní funkci, provádí školení a řešení případných sporů. Zabývá se formálním vydáváním standardů, působí jako RFC editor. Zastřešuje činnost dalších organizací (IETF, IRTF, ICANN atd.).

IESG[19] (INTERNET ENGINEERING STEERING GROUP)

Jedná se o organizaci zodpovědnou za technický management IETF a za schvalovací proces internetových standardů. Schvalovací proces provádí dle pravidel ISOC (podrobněji viz. dále).

IRTF[20] (INTERNET RESEARCH TASK FORCE)

IRTF je organizace zaměřená na vědu a výzkum. Jejím hlavním zaměřením je orientace na vývoj a budoucnost Internetu, protokolů, aplikací, architektury a internetových technologií.

---

[16] ISOC. *Internet Society* [online]. [vid. 15. Prosince 2013]. Dostupné z: http://www.internetsociety.org/
[17] IETF. *Internet Engineering Task Force* [online]. [vid. 15. Prosince 2013]. Dostupné z: http://www.ietf.org/
[18] IAB. *Internet Architecture Board* [online]. [vid. 15. Prosince 2013]. Dostupné z: http://www.iab.org/
[19] IESG. *Internet Engineering Steering Group* [online]. [vid. 15. Prosince 2013]. Dostupné z: http://www.ietf.org/iesg/
[20] IRTF. *Internet Research Task Force* [online]. [vid. 15. Prosince 2013]. Dostupné z: http://irtf.org/

IANA[21] (INTERNET ASSIGNED NUMBERS AUTHORITY)

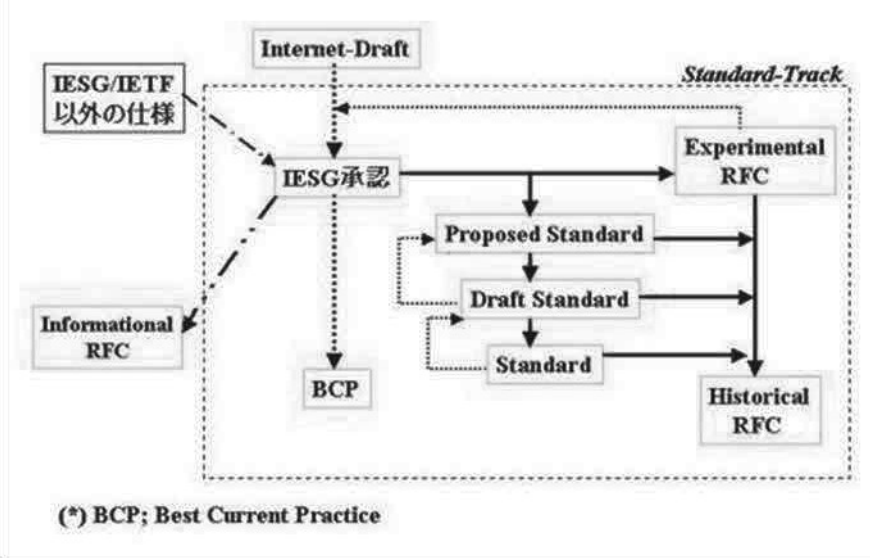
Organizace zabývající se správou doménových jmen a IP adres. V této oblasti má také na starosti vývoj a koordinaci celého procesu.

ICANN[22] (INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS)

Organizace, která zastřešuje činnost regionálních registrátorů doménových jmen. Spolupracuje s organizací IANA.

4.5 Internetové standardy

Internetové standardy jsou dokumenty, které mají za cíl přispívat k procesu koordinace vývoje internetu a internetových technologií jako takových. Jejich význam je především ve sjednocování procesu komunikace mezi jednotlivými, často velmi odlišnými technologiemi, ať už v rovině hardwarové či softwarové. Standardy vznikají z tematicky sdružených RFC dokumentů, které prošly mnohdy náročným schvalovacím procesem (standard track).



Obrázek 48: RFC Standard Track

Zdroj: Botlík, Slaninová, 2014, Služby Internetu a internetové systémy, výukový materiál OPF v Karviné

[21] IANA. *Internet Assigned Numbers Authority* [online]. [vid. 15. Prosince 2013]. Dostupné z: http://www.iana.org/
[22] ICANN. *Internet Corporation For Assigned Names And Numbers* [online]. [vid. 15. Prosince 2013]. Dostupné z: http://www.icann.org/

4.5.1 RFC (REQUEST FOR COMMENT) DOKUMENTY

RFC dokumenty jsou dokumenty vydávané organizací IETF, zaměřené na metody, chování, výzkum a inovace aplikovatelné v prostředí internetu. Dokumenty jsou jednoznačně číslovány, jsou volně šiřitelné a dostupné pro širokou veřejnost na internetu.

Existují tři základní kategorie RFC dokumentů. První a nejdůležitější kategorií jsou **Standardy** – nejdůležitější kategorie. Dělí se dále na:

- *Proposed Standard* - počáteční úroveň, kdy ještě neexistuje dostatek zkušeností z praxe. Dokument sice může být kompletní z hlediska specifikace, jsou ale možné změny po stránce implementační či aplikační, např. RFC2535 (první definice DNSSEC),
- *Draft Standard* – dokumenty, na které jsou kladeny již větší nároky jak po stránce implementační, tak po stránce dostatečných zkušeností s provozem, např. specifikace směrovacího protokolu BGPv4,
- *Standard* – finální úroveň standardizace. RFC, které se dostane schvalovacím procesem až do kategorie Internet Standard, je již propracovaným a plně vyzrálým dokumentem. Jako příklad můžeme uvést poštovní protokoly SMTP a POP3, specifikaci kódování UTF-8 a mnoho dalších.

Dále existují tzv. ne-standardy, což jsou dokumenty, které z různých důvodů neprošly řádně schvalovacím procesem. Jedná se o dokumenty **Experimentální**, **Informativní** a **Historické**.

Poslední kategorií jsou dokumenty **BCP** (Best Current Practice), což jsou RFC dokumenty obsahující popis nejlepší současné praxe. Nedefinují tedy žádný konkrétní standard, ale působí jako jakýsi návod.

Podíváme-li se např. na oblast tvorby webu, nemůžeme zde nezmínit organizaci W3C[23] (World Wide Web Consortium), která se v této oblasti angažuje nejvíce. Zakladatelem této organizace, a v současné době také výkonným ředitelem je Tim Berners-Lee, zakladatel WWW. V této oblasti se setkáme hned s několika standardy. Již samotné zobrazování stránek a World Wide Web jako takový funguje na principu protokolu HTTP, který je také standardem, nemluvě o protokolech dalších, jako jsou TCP/IP využívaný v internetové síti, POP3 a SMTP pro zasílání pošty, FTP pro nahrávání (upload) a stahování (download) souborů apod. Při vytváření samotných webových stránek se rovněž vychází ze standardů, většinou příslušných zvolenému jazyku pro tvorbu webu. Mezi jinými zde můžeme zmínit např. HTML a XHTML jako základní jazyky pro tvorbu webu, XML jako formát pro přenos dat, CSS pro formátování a používání stylů, JavaScript jako zástupce skriptovacích jazyků na straně klienta, různé formáty pro multimédia (PNG, SVG, SMIL), MathML pro

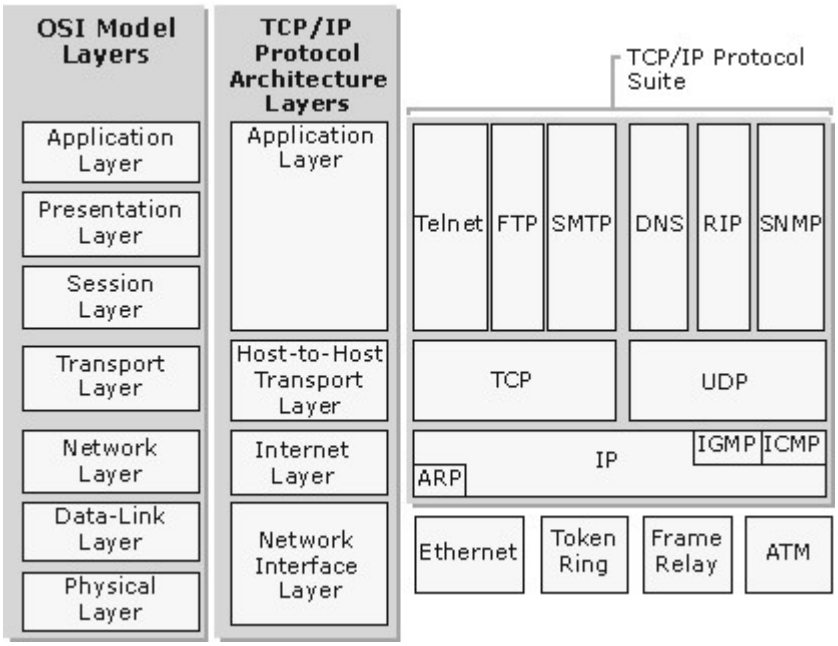
[23] W3C. *World Wide Web Consortium* [online]. [vid. 15. Prosince 2013]. Dostupné z: http://www.w3.org/

vkládání matematiky na web a další. Existuje další řada standardů, používaných v této oblasti, např. standardy týkající se přístupnosti webu (WCAG), standardy pro mobilní aplikace, pro různá zařízení přistupující k webu atd. Nebudeme zde rozebírat podrobně jednotlivé standardy, pouze je v následujících kapitolách zmíníme, pokud to bude nutné.

4.6 Síťové modely

Princip Internetu je založený protokolech, které zabezpečují komunikaci na několika „vrstvách“. Zjednodušeně řečeno, aplikace se mezi sebou snaží domluvit. Komunikace probíhá na vrstvě „aplikační komunikace“. Nepodaří-li se jim z nějakého důvodu zabezpečit vzájemnou komunikaci (např. nedostupnost počítače nebo neúplná znalost pravidel), obrátí se na další vrstvu, svá data „zabalí“ do balíčku, který předají této vrstvě a požádají tuto vrstvu o přenos. tohoto je zřejmé, že v prostředí internetu je několik komunikačních vrstev a na těchto vrstvách probíhají různé formy komunikace a přenosu dat. Ve většině služeb fungujících na Internetu pak komunikace probíhá tak, že jeden počítač poskytuje prostředky a určuje pravidla a jiný prostředky využívá, tj. komunikace probíhá na úrovni server – klient, viz Kapitola 3.4. Tento princip umožňuje pak komunikaci v heterogenním prostředí různých sítí, operačních systémů či hardware.

Pro vysvětlení, jakým způsobem komunikace v jednotlivých vrstvách sítě funguje, se velmi často používají tzv. síťové modely. Existují dva základní modely: model založený na rodině protokolů TCP/IP a referenční ISO/OSI model. Jelikož je daná problematika velmi obsáhlá a detaily jsou náplní jiného předmětu, vysvětlíme v této části publikace jen stručně základní principy. Srovnání obou těchto modelů je uvádí **Chyba! Nenalezen zdroj odkazů.**.

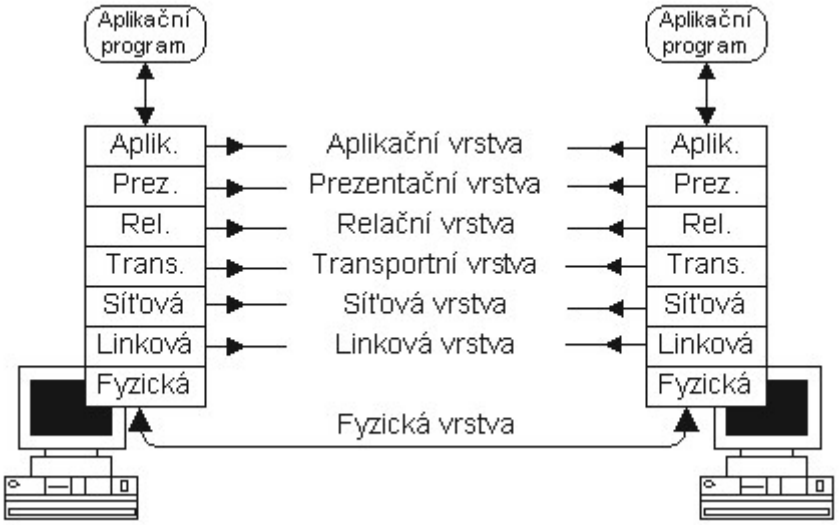


Obrázek 49: Srovnání síťových modelů

Zdroj: [online]. [vid. 1.9 2013]. Dostupné z: http://technet.microsoft.com/en-us/library/cc958821.aspx

4.6.1 ISO/OSI MODEL

Referenční model ISO/OSI vzniknul na základě snahy organizace ISO o standardizaci počítačových sítí. Tento model byl pak v roce 1984 přijat jako mezinárodní norma ISO 7498. Cílem tohoto modelu bylo poskytnout základ pro další normy, které slouží pro propojování systémů. Není zde tedy přímo specifikována samotná implementace systémů, ale jsou zde uvedeny principy pro základní komunikaci v síti pomocí sedmi vrstev. Na rozdíl od TCP/IP modelu nezahrnuje žádné protokoly a další detaily. V praxi se tento model využívá při programování jednotlivých součástí síťových rozhraní.



Obrázek 50: ISO/OSI model

Zdroj:Kabelová, Dostálek, 2010

Komunikace mezi vrstvami jednoho systému se pak řídi pravidly, která jsou nazývána jako rozhraní (interface). Komunikace mezi stejnými vrstvami různých systémů (zařízení) se pak nazývají podobně jako u TCP/IP modelu protokoly.

Jak již bylo zmíněno, model obsahuje sedm vrstev: fyzickou (*physical layer*), linkovou (*data link layer*), síťovou (*network layer*), transportní (*transport layer*), relační (*session layer*), prezentační (*presentation layer*) a aplikační (*application layer*).

Fyzická vrstva

Nejnižší, fyzická vrstva je zaměřena na fyzickou komunikaci v síti. Je zaměřena na fyzikální a elektrické vlastnosti zařízení, vlastnosti kabelů, stanovuje způsob přenosu. Hlavními funkcemi této vrstvy je navazování a ukončování spojení, modulace digitálních dat na signál používaný přenosovým médiem a efektivní rozložení zdrojů mezi uživatele v síti. Na této vrstvě pracují např. HUBy, opakovače a síťové adaptéry.

Linková vrstva

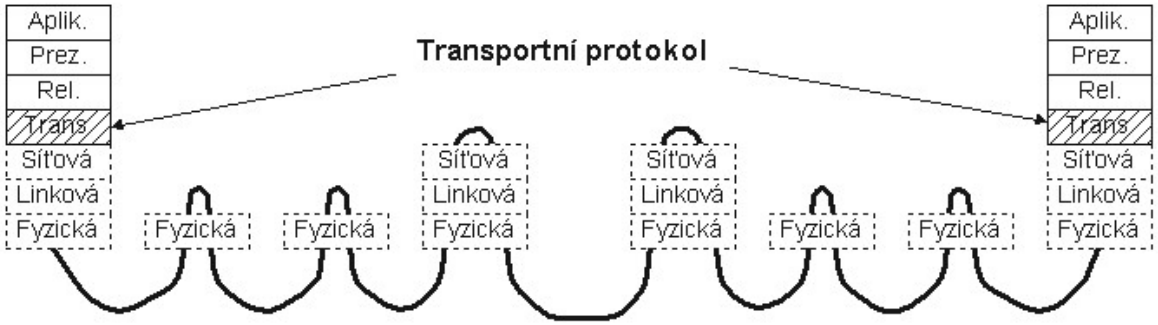
Linková vrstva má na starosti spojení mezi dvěma sousedními systémy. Definuje nastavení parametrů přenosu linek, oznamuje chyby. Na této vrstvě pracují např. mosty a přepínače.

Síťová vrstva

Tato vrstva má na starosti adresaci v síti. Zajišťuje tak spojení mezi systémy, které spolu bezprostředně nesousedí. Poskytuje směrovací funkce a stará se o doručení dat. Na této vrstvě tedy pracují např. směrovače. Můžeme zde zmínit také protokol IP, který pracuje na této vrstvě. Na síťové vrstvě je jednoznačně v celé WAN adresováno síťové rozhraní. Síťovým rozhraním může být např. karta pro Ethernet.

Transportní vrstva

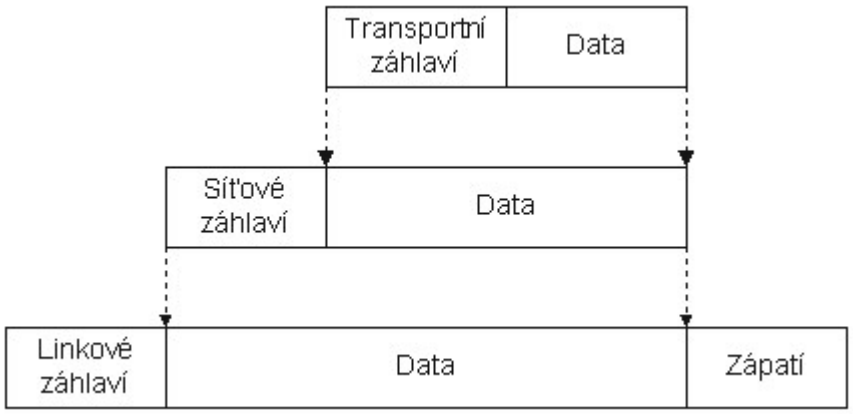
Transportní vrstva pak zajišťuje přenos dat mez koncovými uzly. Její hlavní funkcí je starat se o kvalitu přenosu na takové úrovni, kterou vyžadují vyšší vrstvy. Můžeme se zde setkat se dvěma základními protokoly, spojově orientovaným TCP a nespojově orientovaným UDP.



Obrázek 51: Spojení na transportní vrstvě

Zdroj:Kabelová, Dostálek, 2010

Mezi dvěma počítači může být několik transportních spojení současně, jedno např. pro virtuální terminál a druhé pro elektronickou poštu. Aplikace jsou jednoznačně adresovány v rámci jednoho počítače. Jednotkou přenosu je transportní paket, který se opět skládá ze záhlaví a datové části. Transportní paket se přenáší v datové části síťového paketu.



Obrázek 52: Spojení na transportní vrstvě

Zdroj:Kabelová, Dostálek, 2010

Relační vrstva

Relační vrstva se stará o organizaci a synchronizaci mezi relačními vrstvami dvou systémů a řídí výměnu dat mezi nimi. Jedná se tedy o vytvoření a ukončení relačního spojení, synchronizaci a obnovení spojení apod. Na této vrstvě se můžeme setkat s protokoly jako NetBIOS, AppleTalk, SSL, RPC a další.

Prezentační vrstva

Na této vrstvě jsou pak data prezentována do tvaru, který používají aplikace. Jedná se např. o šifrování, konvertování nebo komprimaci. Vrstva je definována z důvodu možného rozdílu formátu dat při komunikaci různých aplikací na obou stranách. Vrstva se zaměřuje na strukturu dat, jejich význam pak přenechává vrstvě aplikační.

Aplikační vrstva

Na vrstvě aplikační se pak setkáme s protokoly umožňující komunikaci mezi aplikacemi a komunikačním systémem. Protokolů fungujících na této vrstvě je celá řada, můžeme zde uvést např. FTP, DNS, POP3, SMTP, DHCP, SSH a další.

4.6.2 TCP/IP MODEL

TCP/IP model je založen na rodině protokolů TCP/IP. Jeho vznik můžeme datovat do počátků sedmdesátých let devatenáctého století. Bývá také často nazýván jako *internet model*. Definuje čtyři kategorie funkcí, které musí být provedeny, aby byla komunikace na internetu úspěšná. Jedná se o otevřený standard, není tedy závislý na jedné instituci či firmě. Protokoly kolekce TCP/IP jsou veřejně posuzovány a diskutovány (byly především při jejich vzniku a průběžně vznikají další) prostřednictvím RFC dokumentů, viz Kapitola 4.5.

RFC dokumenty zahrnují také technické a organizační dokumenty týkající se internetu jako takového, včetně technických specifikací.

V TCP/IP modelu jsou definovány čtyři základní vrstvy, které znázorňují hierarchii činností. Mezi těmito vrstvami je přesně definována výměna informací, přičemž každá vrstva využívá služeb vrstvy nižší a poskytuje své služby vrstvě vyšší. Jedná se o tyto vrstvy: aplikační (*application layer*), transportní (*transport layer*), síťová (*internet layer*) a vrstva síťového rozhraní (*network interface*). Komunikace mezi stejnými vrstvami je pak řízena tzv. komunikačními protokoly.

VRSTVA SÍŤOVÉHO ROZHRANÍ

Tato nejnižší vrstva umožňuje přístup k fyzickým médiím umožňujícím komunikaci v síti. Je samozřejmě specifická pro každou síť, podle její implementace. Jako příklad zde můžeme uvést např. Ethernet, Token ring, FDDI, X.25, SMDS a další.

SÍŤOVÁ VRSTVA

Síťová vrstva má na starosti síťovou adresaci, předávání tzv. datagramů a jejich směrování. Na této vrstvě se můžeme setkat s protokoly IP, ARP, ICMP a dalšími.

TRANSPORTNÍ VRSTVA

Transportní vrstva je pak implementována až v koncových zařízeních přistupujících k internetu. Poskytuje transportní služby prostřednictvím protokolu TCP (*transmission control protocol*) nebo méně spolehlivým protokolem UDP (*user datagram protocol*).

APLIKAČNÍ VRSTVA

Z hlediska služeb internetu nás bude zajímat nejvíce poslední vrstva, vrstva aplikační. Jedná se o vrstvu, která má na starosti procesy aplikací využívajících přenosu dat po síti pro poskytování konkrétních služeb. Jako příklad zde můžeme uvést FTP, HTTP, DHCP, Telnet, DNS, POP3, SMTP a další. Některé ze zmiňovaných služeb budou podrobněji rozebrány v následujících kapitolách.

SHRNUTÍ KAPITOLY

V této kapitole jste se seznámili se základy fungování Internetu, zejména s protokolem TCP/IP a jeho jednotlivými vrstvami. Dále jste se seznámili s protokoly aplikační vrstvy a službami provozovanými na této vrstvě.

5 PILÍŘE A ORGANIZACE INTERNETU, WWW

RYCHLÝ NÁHLED KAPITOLY

V této kapitole bude představen základní koncept Internetu, tři stěžejní pilíře na kterých je internet postaven. Studenti se seznámí s organizací a přidělováním IP adres a doménových jmen a s fyzickou infrastrukturou.

CÍLE KAPITOLY

Cílem kapitoly je seznámit studenty se základními pojmy, se kterými se setkají při práci s Internetem, zejména s hlavními pilíři. Studenti se blíže seznámí s fyzickou strukturo, vztahem mezi doménami a IP adresami a přidělováním doménových jmen a IP adres

ČAS POTŘEBNÝ KE STUDIU

Čas potřebný ke studiu v rozsahu 3-5 hodin, podle míry praktické práce.

KLÍČOVÁ SLOVA KAPITOLY

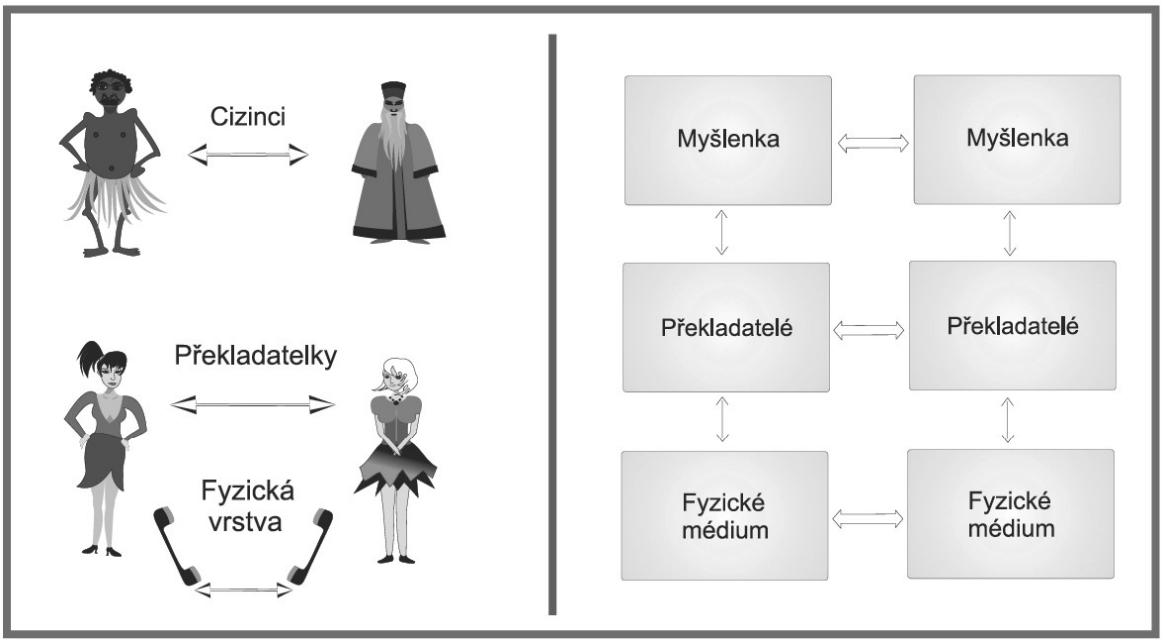
ISP, URL, DNS, doména, infrastruktura, Cesnet

5.1 Tři pilíře Internetu

Dá se jednoduše shrnout, že Internet má 3 základní pilíře, na kterých je postaven. V první řadě je to komunikační protokol TCP/IP, dále systém doménových adres a v neposlední řadě fyzická infrastruktura.

5.1.1 KOMUNIKAČNÍ PROTOKOLY

Komunikační protokoly tvoří jeden ze základních stavebních kamenů Internetu. Vzhledem k multiplatformnímu prostředí Internetu je nutné zabezpečit taková komunikační pravidla, která konečným počtem standardizovaných kroků zabezpečí komunikaci. Dostálek a Kabelová (2012) přirovnávají komunikaci k rozhovoru dvou vzdálených cizinců. Každý umí mluvit, ovládá proto komunikační protokol. Každý má však tento protokol odlišný (např. čeština, francouzština). Komunikace tedy teoreticky probíhá mezi cizinci, prakticky však cizinci musí předat komunikaci jiné komunikační vrstvě, která „má stejný protokol" – tlumočnicím.



Obrázek 53: Třívrstvá komunikační architektura

zdroj: Kabelová, Dostálek (2012)

Prakticky tedy cizinci nehovoří spolu ale s tlumočnicemi. Pokud nejsou tlumočnice „v kontaktu", nemohou se tedy domluvit, sáhnou opět po další komunikační vrstvě. Teoreticky tedy hovoří spolu tlumočnice, prakticky však každá tlumočnice hovoří „s telefonem". Takto může být komunikace definovaná na více vrstvách, musí však být zabezpečené, že se na některé vrstvě komunikace uskuteční (definovaný konečný počet vrstev).

Komunikace mezi počítači (obecněji mezi aktivními síťovými prvky) v prostředí Internetu je založena na protokolu TCP/IP.

5.1.2 FYZICKÁ INFRASTRUKTURA

Aby mohla komunikace mezi počítači v Internetu probíhat, musí být k dispozici komunikační kanály, musí být vytvořena komunikační (síťová infrastruktura).

Internet využívá množinu takovýchto infrastruktur, jejichž provozovatelé (provideři) umožňují připojení uživatelů do sítě. Propojení sítí se realizuje prostřednictvím peeringu. Peering je pojmenování pro vzájemné propojení počítačové sítě dvou různých (např. telekomunikačních) společností za účelem výměny datového provozu na centrálních místech (exchange points) individuálně nebo hromadně. Výsledkem vzájemného propojení všech takových sítí po celém světě je tedy Internet (celosvětová síť). Peeringové uzly jsou páteří celého Internetu. Peering může být privátní - přímé propojení sítí dvou ISP nebo veřejný (public) - hromadné propojení více sítí v jednom místě.

V praxi se pro označení Peeringových uzlů používají zkratky IXP – Internet Exchange Point[24], NAP – Network Access Point, MAE – název společnosti Metropolitan Area Exchange, který se v USA vžil pro generické označování NAPs, aj. V rámci evropského prostoru se nejčastěji používá označení IXP. IXP je fyzickým místem, ve kterém si ISPs (Internet Service Providers) a CPs (Content Providers) vyměňují své datové toky. IXP snižuje společnostem náklady na zahraniční konektivitu. Analogií může být letiště-dopravní křižovatka (IXP), kde pasažéři (datové balíčky), přestupují, vystupují a nastupují do a z letadel různých dopravních společností (ISP, CP). Z pohledu provozovatele lze rozdělit IXP na 2 kategorie:

•Nekomerční IXP – asociace, neutrální organizace, kde vloženými penězi (ve formě poplatků za využívání IXP) sdružené společnosti financují provoz svého IXP.

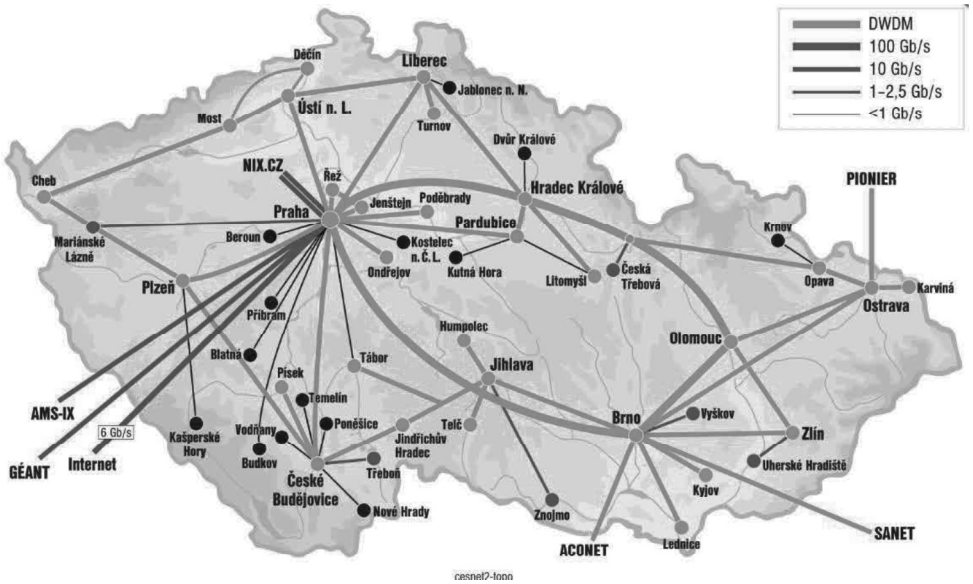
•Komerční IXP – provozovatelem je soukromá firma, ISP jsou její zákazníci a poplatky platí provozovateli.

V Evropě jsou rozšířeny spíše nekomerční IXP, v USA převládá kategorie komerčních IXP. Obě kategorie mají své klady a zápory. V nekomerčním IXP sdružené společnosti samy rozhodují o vývoji, strategii, cenách a investicích svého IXP, naproti tomu v komerčním IXP platí zainteresované společnosti za služby poskytovateli služeb, který může být přímým konkurentem, a mají pouze dvě možnosti v rozhodování, a to sice buď služby odebírat, nebo neodebírat. Na druhé straně v nekomerčním IXP mají sdružené společnosti i příslušný díl zodpovědnosti za svá rozhodnutí a konsenzus společností musí projít diskuzí a zpravidla v některých IXP hlasováním, zatímco komerční IXP dělá rozhodnutí dle svého uvážení, což umožňuje pružnější reakci na podněty z vnějšího okolí.

Mezi významná veřejná peeringová centra patří NIX.CZ. V současné době je sdružení největším neutrálním IXP v České republice a řadí se mezi deset největších IXP v Evropě. Sítě připojené k platformě NIX.CZ mají možnost propojení s dalšími připojenými sítěmi ISP (Internet Service Providers) nebo IAP (Internet Access Provider). NIX.CZ patří mezi nekomerční IXP kde členové hlasují o ceníku, rozpočtu, vzniku/zániku nových uzlů, a volí statutární orgány.

[24] Zdroj: http://www.lupa.cz/clanky/nix-cz-minulost-soucasnost-a-budoucnost/

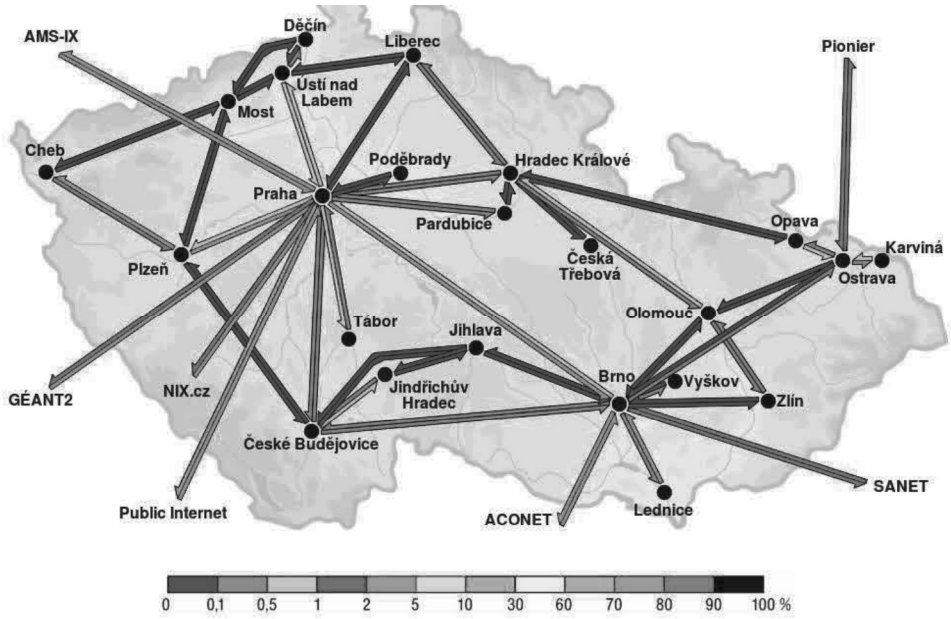
Slezská univerzita využívá sítě TEN společnosti Cesnet. Síť Cesnet je součástí struktury Geant.



Obrázek 54: topologie sítě Cesnet

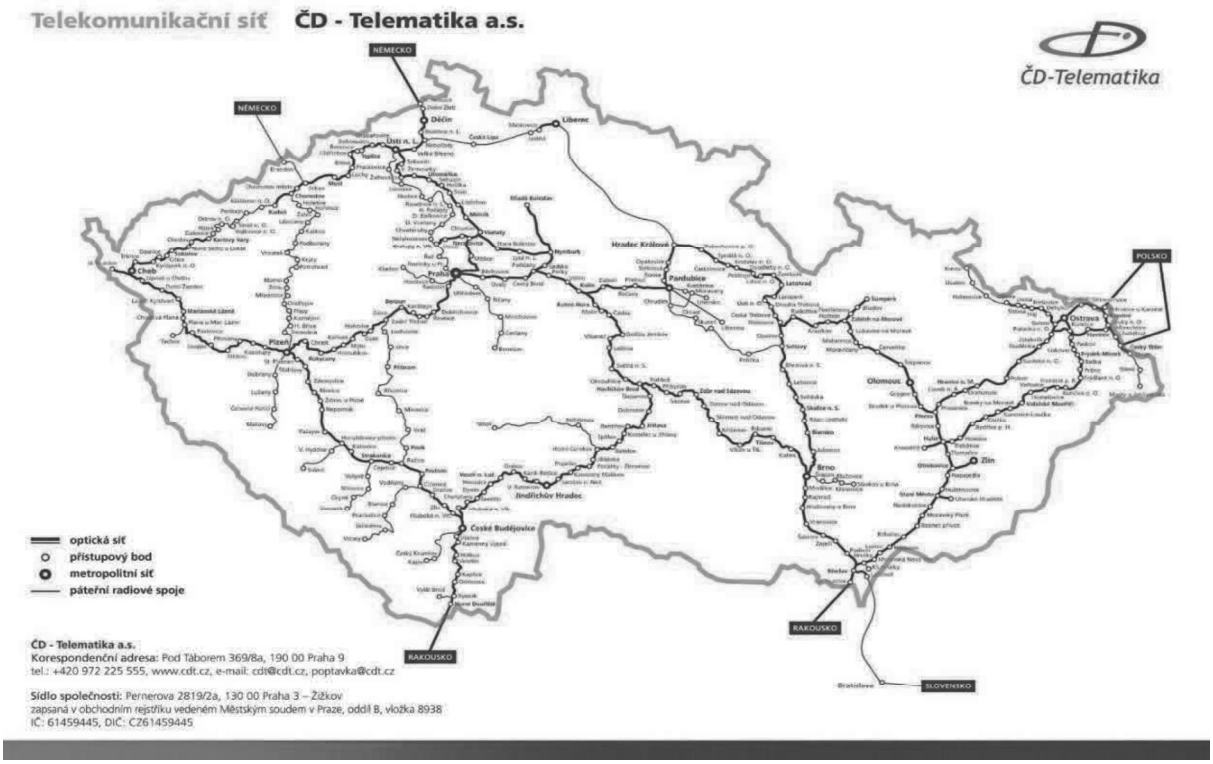
Zdroj: [online]. [vid. 1.9 2013]. Dostupné z:http://www.cesnet.cz/sluzby/pripojeni/topologie/

Na stránkách cesnet.cz jsou veškeré záležitosti týkající se této infrastruktura, včetně realizovaných propojení, projektů nebo např. aktuálního zatížení sítě.



Obrázek 55: Ukázka zatížení jednotlivých tras sítě Cesnet

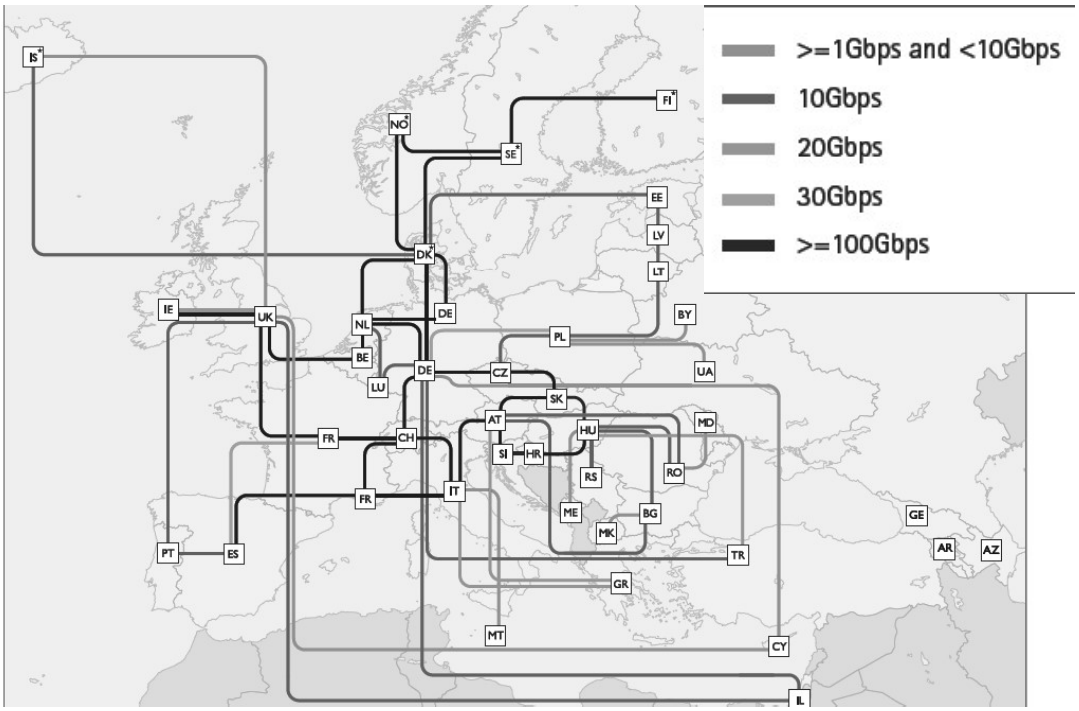
Zdroj: [online]. [vid. 1.9 2013]. Dostupné z: http://netreport.cesnet.cz/netreport/



Obrázek 56: ukázka topologie sítě ČD-Telematika

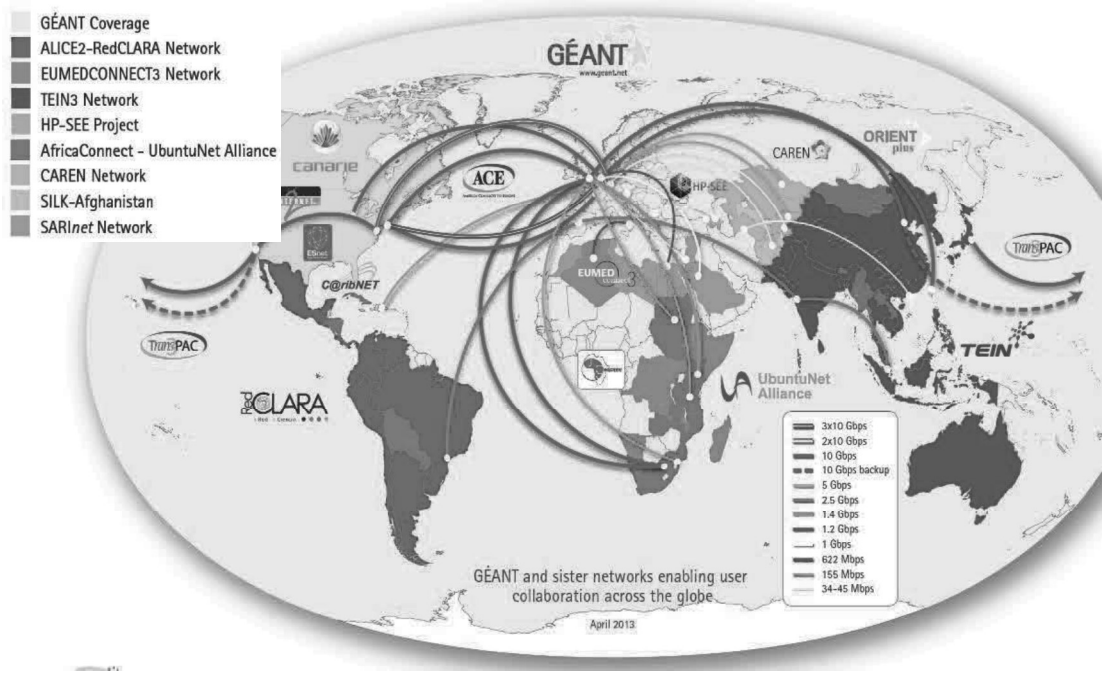
Zdroj: [online]. [vid. 1.9 2013]. Dostupné z:http://www.cdt.cz/cz/infrastruktura-97/

V rámci konektivity se sítě propojují i v rámci států, resp. vytvářejí se nadnárodní struktury. Příkladem může být Geant – Pan evropská síť pro vědu a vzdělávání.



Obrázek 57: Pan evropská síť pro vědu a vzdělávání

Zdroj: Cesnet, [online]. [vid. 1.9 2013]. Dostupné z: www.geant.net



Obrázek 58: Světová konektivita - Geant

Zdroj: [online]. [vid. 1.9 2013]. Dostupné z: http://www.geant.net/Resources/Media_Library/Pages/Maps.aspx

5.1.3 DOMÉNY

Třetím pilířem Internetu je systém doménových adres. Na základě přidělování IP adres a doménových adres je vytvořena struktura doménových jmen, kdy každá doménová adresa je ve své podstatě „jinak zapsaná“ IP adresa příslušného počítače. Identifikaci (překlad adres) zabezpečují DNS servery na základě protokolu DNS. Blíže se doménám věnují kapitoly později.

5.2 Fungování internetu

Internet je v podstatě rozsáhlá počítačová síť, která vzniká propojením několika stovek sítí. Internet je tedy spousta spojených počítačů, pokud se však propojí několik počítačů, ještě to neznamená, že máte dílčí mini internet.

K tomu, aby informace byly vidět je potřeba mít na minimálně jednom počítači internetový server. Internetový server je tedy opět počítač, který umožní sdílet určité informace okolnímu světu. Opakem je klient. Klientem je každý počítač, co je připojen k internetu a má nainstalovaný prohlížeč[25]. Zjednodušeně řečeno tedy pokud spustíme prohlížeč, tak ten se nám připojí k nějakému serveru a zobrazí nám informace, které na tom serveru jsou. To, o který server se jedná, je určeno jeho adresou. Každá tato adresa je jedinečná a v internetu nemohou být dvě stejné.

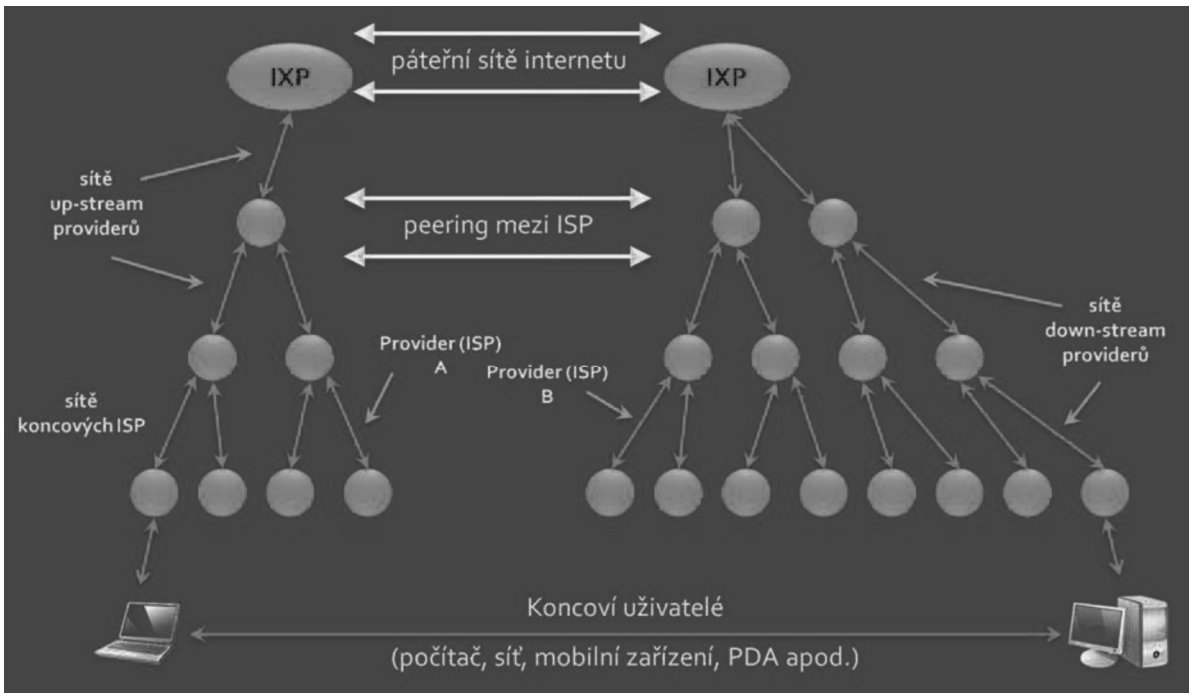
Pojem Internet (složenina předpony inter vyjadřující vztah mezi, a anglického net označujícího síť) se v tomto případě vysvětluje jako celosvětový systém navzájem propojených počítačových sítí, které propojují tzv. síťové uzly. Uzlem pak může být počítač nebo zařízení se speciální síťovou funkcí, například router. Klíčovou pro fungování Internetu, jak jej známe dnes, je také rodina protokolů TCP/IP[26].

Tyto dílčí sítě jsou provozovány subjekty (organizacemi), často nazývanými ISP (Internet Service Provider), tedy poskytovateli připojení. Tito poskytovatelé připojení vytvářejí fyzické propojení počítačů v internetu, přičemž často nabízejí také další služby s touto oblastí spojené. Jak je patrné z následujícího obrázku, tyto subjekty poskytují připojení také

[25] http://www.zasedalsiblog.cz/zjednodusena-struktura-internetu

[26] Co Internet není? (podle http://www.jaknainternet.cz/page/1795/struktura-internetu/)
Obvykle bývá internet zaměňován za internetové stránky, prohlížeč, součást vybavení počítače či telefonu nebo určitou on-line službu. Někdy z neznalosti, častěji ale spíše ze snahy zobecnit význam pojmu Internet, aby lépe odpovídal tomu, jak jej známe z běžného života. Lze tedy rozlišovat mezi Internetem v užším a širším slova smyslu.
WWW stránky, e-mail atd. (Internet podle laika), jsou jen některé z tzv. služeb, které je možné na Internetu provozovat. Tyto služby zajišťují počítačové programy, které mezi sebou komunikují pomocí protokolů (protokoly jsou definovány jako seznam doporučení, jejichž dodržování vede k bezproblémovému fungování služeb). Další známé internetové služby jsou například instant messaging (protokoly ICQ, Jabber…), VoIP - internetová telefonie (protokol SIP, proprietární, tedy uzavřený protokol Skype…), přenos souborů (FTP) atd.

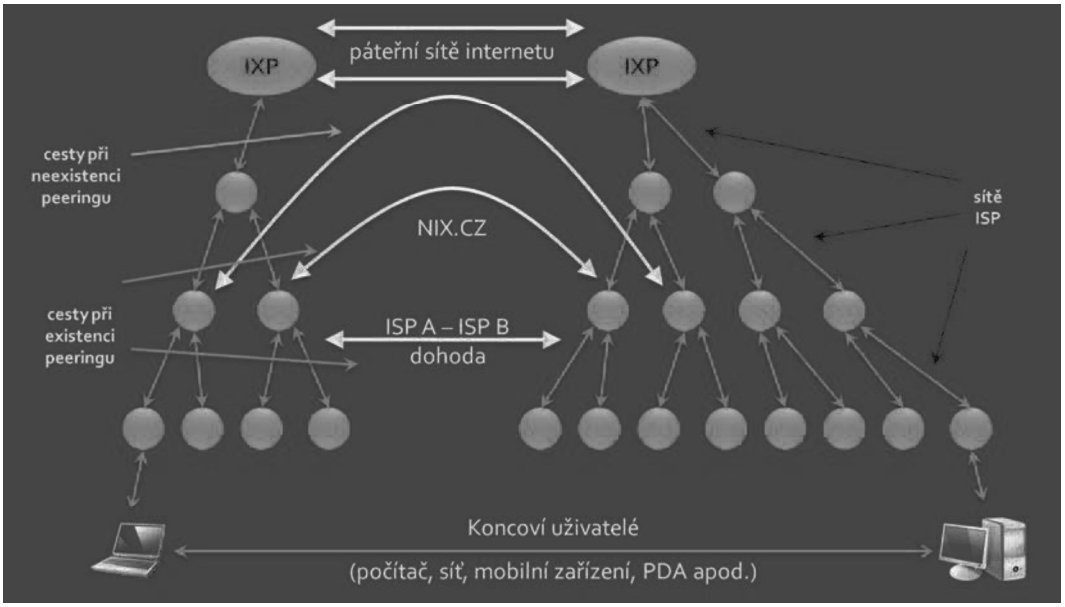
dalším subjektům. Pokud bychom se na toto jednoduché schéma dívali z pohledu hierarchie, budeme o větších poskytovatelích, resp. o jejich sítích, hovořit jako o sítích up-stream providerů. Tyto subjekty pak připojují menší subjekty, resp. jejich sítě (down-stream sítě providerů). Na obrázku jsou znázorněny tyto sítě obousměrnými šipkami. Na nejnižší úrovni této pomyslné hierarchie pak nalezneme sítě koncových providerů, tedy sítě poskytovatelů připojení, kteří do internetu fyzicky připojují koncové uživatele.



Obrázek 59: Zjednodušené schéma internetu

Zdroj: Botlík, Slaninová, 2014, Služby Internetu a internetové systémy, výukový materiál OPF v Karviné

Rychlost připojení v rámci jednotlivých sítí jednotlivých poskytovatelů připojení se liší v závislosti na použité technologii a v závislosti na jejich propojení se sítěmi ostatních poskytovatelů připojení. Ve skutečnosti internetová síť nevypadá takto jednoduše hierarchicky, byť zřejmě k nejrychlejšímu propojení dochází stále přes páteřní síť internetu, ke které jsou prostřednictvím přípojných bodů nazývaných IXP (Internet Exchange Point) připojeni největší poskytovatelé připojení. Konektivita, tedy rychlost spojení mezi dvěma body v internetu (někdy také rychlost připojení dané sítě vzhledem k určenému cíli), je dána způsobem propojení jednotlivých sítí mezi sebou.



Obrázek 60: Zjednodušené schéma internetu – peering

Zdroj: Botlík, Slaninová, 2014, Služby Internetu a internetové systémy, výukový materiál OPF v Karviné

Obrázek ukazuje, že v případě nepropojených sítí dvou poskytovatelů připojení, např. A a B, by data od koncového uživatele musely cestovat nejprve v rámci hierarchie sítě poskytovatele A až k páteřní síti internetu, a pak opět shora dolů v rámci hierarchie až k poskytovateli B. Konektivita je pak dána nejslabším článkem v rámci této cesty, tedy nejpomalejším spojením (opět dáno použitými technologiemi, často nejpomalejší spojení je mezi koncovým uživatelem a koncovým ISP, např. bluetooth, wi-fi spojení, či modem). Z důvodu zkrácení těchto cest a samozřejmě z důvodu urychlení přenosu informací dochází k propojování sítí jednotlivých ISP na nižší úrovni. Toto propojování je prováděno na základě bilaterálních dohod, popř. je zastřešováno organizacemi v rámci jednotlivých IXP (Internet Exchange Point). Tyto výměnné body pak poskytují infrastrukturu pro propojení jednotlivých sítí autonomních systémů jednotlivých ISP. V České republice působí zájmové sdružení ISP právě s cílem propojení sítí jednotlivých poskytovatelů připojení s názvem NIX.CZ[27] (Neutral Internet eXchange.

5.2.1 Služby ISP

Poskytovatelé připojení v současné době kromě samotného fyzického připojení nabízí také další služby, jako např. web hosting, server hosting, registraci doménových jmen, tvorbu webových stránek a vývoj internetových aplikací, správu databází či další služby (VoIP, vyhledávací služby, mail servery apod.).

[27] NIX.cz, z.s.p.o. *Neutral Internet eXchange* [online]. [vid. 15. Prosince 2013]. Dostupné z: http://www.nix.cz

Také dochází s nástupem digitalizace k prolínání dvou, dříve samostatných, světů počítačových sítí a telekomunikací. Dochází jak ke konvergenci sítí, tak poskytovaných služeb. Není dnes výjimkou, že poskytovatel připojení, počítačová firma, poskytuje služby v oblasti IP telefonie (VoIP), že se setkáváme s televizním a rozhlasovým vysíláním po internetu (IPTV), že internetové připojení nabízí kabelové televizní společnosti apod.

5.2.2 TIER

Obecně se velké sítě dělí podle své velikosti do tříd zvaných „Tier“. „Tier 1 jsou společnosti, které stály u zrodu internetu nebo byly velkými operátory na důležitých trzích. Tyto sítě se mezi sebou propojují zdarma a ostatní od nich musí ‚nakupovat internet‘,“[28]. Společností s označením Tier 1 je jen okolo patnácti. „Typicky jsou globální, mají tedy přípojné body na všech kontinentech.“

Dalším zajímavým prvkem internetu jsou takzvané Content Delivery Network (CDN), což jsou sítě pro rozložení zátěže pro distribuci software a jiných dat. Zlepšují uživatelský konfort, protože umožňují stahovat obsah z nejbližšího úložiště. Mezi nejznámější sítě patří Akamai, Amazon nebo Limelight. „Pokud by takové sítě neexistovaly, docházelo by k přetížení nejen u samotných serverů, ale i třeba na podmořských linkách.“[10]

Všichni poskytovatelé kromě Tier 1 musí nakupovat „tranzit“, tedy připojení do celého internetu. Tranzit se nakupuje buďto za fixní cenu nebo běžnější metodou podle přenesených dat.

5.3 Identifikace souborů a počítačů

Aby byla v prostředí internetu možná komunikace, je nutné vědět, s kým daná komunikace probíhá. To je zajištěno jednoznačnou identifikací všech zařízení a objektů v internetovém (síťovém) prostoru. Jedná se nejen o servery (od webových serverů přes file servery, záložní servery až po koncová zařízení jednotlivých uživatelů. Jako příklad zde můžeme uvést server, na kterém jsou umístěny soubory s www stránkami. WWW stránka je v podstatě soubor nebo množina souborů, které jsou umístěny na disku nějakého počítače (zpravidla serveru, který je přístupný 24 hodin denně, 7 dní v týdnu, 365 dní v roce). Ten, kdo chce zobrazit www stránku, by tedy měl zadat název souboru, který chce zobrazit, jeho umístění na příslušném disku a umístění příslušného počítače. Tyto údaje musí být současně jednoznačné a světově jedinečné, aby se příslušný soubor opravdu našel. Jednou z podmínek pro distribuci www stránek je tedy zřízení jednoznačné adresy, za kterou „schováme“ naše soubory na příslušných discích v příslušných počítačích.

[28] Golecký, A., Lehký úvod do peeringu aneb jak funguje NIX.CZ, přednáška, dostupné na: https://www.root.cz/clanky/lehky-uvod-do-peeringu-aneb-jak-funguje-nix-cz/

5.3.1 URI, URL, URN

Jak bylo zmíněno v předchozím příkladu, potřebujeme tedy pro zobrazení www stránky nějako adresu, na kterou naše dokumenty uložíme a kde si je uživatelé Internetu najdou. Tato adresa musí, obdobně jako „klasická domovní“ adresa splňovat určitá pravidla. V této souvislosti se zjednodušeně někdy místo „adresa“ používá pojem „odkaz“ na soubor, či „URL odkaz“ na soubor. V praxi se pak můžeme setkat s pojmy URI odkaz, URL odkaz a URN odkaz. URI je množina obsahující podmnožiny URL a URN. URI adresa je obecné označení, zatímco URL adresa a URN adresa jsou konkretizující pojmy.

URI

URI (*Uniform Resource Identifier* - jednotný identifikátor zdrojů) představuje způsob, jak identifikovat jednotlivé zdroje v Internetu. Zkratka URI není tolik známá a rozšířená jako URL, jedná se spíše o obecný pojem, který řeší umístění zdroje i jeho pojmenování.

URN

URN (*Uniform Resource Name* -jednotný identifikátor jména) popisuje především název internetového zdroje, nestará se už o jeho dostupnost, resp. cestu k němu.

URL

URL (*Uniform Resource Locator* - jednotný lokátor zdroje) je standardně nejrozšířenější způsob uvádění adresy, často je zaměňován s URI. Běžně se jako URL adresa označuje řetězec znaků, které popisují konkrétní umístění dat. URL adresa popisuje tedy především místo, kde je daný dokument (obecněji data) umístěný. URL adresu může tvořit několik částí, které dohromady vytváří konkrétní adresu umístění dokumentu. URL adresa zpravidla obsahuje doménové jméno a schéma (resp. protokol), dále pak může (ale není to povinné) obsahovat tzv. port (identifikuje službu Internetu: Web, pošta, stahování souborů apod.), název souboru a další parametry. Například „http://www.opf.slu.cz/html/vyuka.htm“ je URL odkaz ukazující na dokument „vyuka.htm“, ten leží v adresáři „html“ na počítači s názvem (s doménovým jménem) „www.opf.slu.cz“. Tento dokument je dostupný pomocí protokolu http, viz Kapitola 4.6.

5.3.2 Doména, IP adresa

Níže uvedený výklad je opět účelově zjednodušený a slouží pro pochopení principu. V předchozí podkapitole je uvedeno, že se v daném URL jedná o název počítače „www.opf.slu.cz“. Přesněji, jedná se o počítač, který je v nějakém prostoru nazvaný www.opf.slu.cz. Tomuto názvu se říká *doména*, resp. *doménové jméno*. Doménové jméno můžeme přirovnat opět ke „klasické“ adrese, v níž jsou jednotlivé údaje odděleny tečkou (příklad: „karel.novak.kosmonautu.karvina.ceska_republika“). Jednotlivé části pak nazýváme domény *k*-tého řádu, přičemž *k* udává pozici zprava a směrem doleva se vždy údaj

upřesňuje a konkretizuje. U www.opf.slu.cz je tedy „cz“ doména prvního řádu, „slu.cz“ je doména druhého řádu (existuje množina domén druhého řádu „XXX.cz“, které jsou podmnožinou domény „cz“), „opf.slu.cz“ je doména třetího řádu (opět existuje množina domén 3. řádu „YYY.slu.cz“, které jsou podmnožinou domény „slu.cz“) atd. Doménu musíme mít, abychom mohli být identifikovatelní. Je to jakýsi „prostor“, ke kterému se návštěvníci našich stránek dostanou a ve kterém máme naše soubory (texty, fotky, videa apod.) potřebné pro naše stránky. Je zřejmé, že někde musíme tento „prostor“ umístit a musíme tento „prostor“ zpřístupnit ostatním. Pokud bychom tento „prostor“ umístili na svém počítači, dobře by se nám stránky vytvářely, protože bychom mohli pracovat na svém počítač. Těžko bychom ale zabezpečili dostupnost našeho počítače pro všechny návštěvníky našich stránek. Přesto je zřejmé, že naše soubory jsou na nějakém počítači. Tento počítač musí být jednoznačně identifikovatelný v prostředí internetu.

Prostředkem pro jednoznačnou identifikaci je tzv. *IP adresa*. Adresa (ve verzi IPv4) má tvar „XXX.XXX.XXX.XXX“ (čtyři tříčíselné části oddělené tečkou), kde XXX je v rozsahu 0 až 255 (např. 193.160.100.100). Tuto adresu má každý počítač v internetu. Aby byla jednoznačně zabezpečená identifikace, jsou tyto adresy přidělovány podle stanovených pravidel. Jednoznačnost IP adresy musí být zabezpečena v rámci uzavřené skupiny, pokud existuje více zařízení se stejnou IP adresou, jsou identifikované skupinou, ve které se nachází (opět je výklad účelově zjednodušený).

Adresa IP se skládá ze dvou částí. Net - ID (adresa sítě) a Host - ID (adresa počítače)[29]. Podle toho jak jsou jednotlivé sítě rozlehlé (kolik mají hostů) rozlišujeme tři hlavní třídy IP adres - A, B a C.

Třída A: dovoluje adresování jen 126 sítí, ale v každé z nich může být až 16 miliónů počítačů. Rozsah hodnot IP adres je: 0.0.0.0 až 127.255.255.255.

Třída B: umožňuje adresovat už 16 tisíc sítí a 65 tisíc počítačů v každé síti. První dva byte je adresa sítě a další dva adresa počítače. V České republice ji mají významné organizace. Rozsah hodnot ve třídě B je: 128.0.0.0 až do 191.255.255.255.

Třída C: umožňuje adresovat až 2 milióny sítí. V každé síti může být 254 počítačů. IP adresa třídy C je v ČR nejpoužívanější. První tři byte jsou adresou sítě a jeden byte adresou počítače. Rozsah je: 192.0.0.0. až 223.255.255.255.

Speciální IP adresy: některé IP adresy jsou vyhrazeny pro speciální účely. Rozsah adres 224.0.0.0 - 239.255.255.255 je zařazen do třídy D a je využívána pro multicasting. Adresy 240.0.0.0 - 247.255.255.255 patří do třídy E, jsou rezervovány. Adresy 127.0.0.0 a 127.0.0.1 jsou tzv. loopback adresy. Pošleme-li data na tuto adresu, nebudou vysílána přes

[29] [online]. [vid. 1.9 2013]. Dostupné z:http://site.the.cz/?id=2, část textu převzata pro výukové účely

žádný ze síťových adaptérů počítače do sítě. Pouze zjistíme, zda je funkční software, nezávisle na tom, funguje-li síťový hardware. Adresu 127.0.0.1 má v podstatě každý počítač, identifikuje lokální počítač.

Síťové adresy jsou adresy, jejichž host část obsahuje samé nuly. Tyto adresy jsou využívány IP protokolem ke správnému směrování paketů mezi sítěmi.

Broadcast adresa, 255.255.255.255 je určena všem hostům v dané síti. Používá se k hromadnému rozesílání paketů.

Pokud je síť izolovaná (Intranet), lze použít libovolné IP adresy. Při připojení vnitřní sítě k Internetu by ale mohla nastat situace, že bude existovat více shodných IP adres. V tomto případě je počítač vnitřní sítě identifikovatelný IP adresou brány. Z důvodů minimalizace konfliktů jsou pro vnitřní sítě rezervované IP adresy 10.0.0.0 až 10.255.255.255 (třída A), 172.16.0.0 až 172.31.0.0 (třída B) a 192.168.0.0 až 192.168.255.0 (třída C).

Jak bylo dříve uvedeno, na zdroje se odkazujeme pomocí doménové adresy. Domény prvního řádu spravuje organizace IANA, viz Kapitola 4.4. Opět velmi zjednodušeně, IANA přidělila České republice doménu 1. řádu „cz“. Současně s touto doménou přidělila k této doméně jistou množinu IP adres např. adresy 193.160.100.0 až 193.160.200.0. Organizace IANA musí současně technicky zabezpečit evidenci přidělených adres k dané doméně a nepřetržitou dostupnost této evidence (tzv. DNS záznamy na DNS serveru). V České republice se o správu domén 2. řádu pod doménou „cz“ a o správu přidělených IP adres stará organizace NIC.cz. Například Slezská univerzita požádala tuto organizaci prostřednictvím registrátora o přidělení domény 2. řádu „SLU.CZ“. Současně s touto doménou dostala SU přidělenou množinu jednoznačných IP adres z množiny přidělených k doméně „cz“ (např. 193.160.200.0 až 193.160.200.200). Organizace NIC opět musí zabezpečit evidenci přidělených adres a domén. Na Slezské univerzitě je OPF, FPF, FVP a Matematický ústav. Tyto součásti dostali od správce domény „slu.cz“ přiděleny domény 3. řádu „opf.slu.cz“, „fpf.slu.cz“, „fvp.slu.cz“ a „mu.slu.cz“. Současně byly opět přiděleny skupiny IP adres a vede se evidence těchto domén a přidělených adres (např. OPF dostane adresy 193.160.200.0 až 193.160.200.20). Správci na Slezské univerzitě disponují tedy těmito adresami a zřídí webový server se jménem „www.opf.slu.cz“ a adresou „193.160.200.1“ (uvedené adresy jsou jen jako příklad).

Napíše-li uživatel do internetového prohlížeče odkaz „www.opf.slu.cz/index.htm“, přeloží se na příslušném DNS serveru toto doménové jméno na příslušnou IP adresu, najde se příslušný počítač o dané IP adrese a v příslušném počítači soubor „index.htm“.

5.3.3 WWW KLIENT

Klient (browser, prohlížeč) je v podstatě prostředníkem mezi uživatelem a WWW serverem. Má na starosti tři **základní činnosti**:

1. Komunikace s uživatelem – jedná se o činnost na základě uživatele, např. vyžádání webových stránek (případně dalších souborů) od WWW serveru, přehrávání multimediálních souborů. Pro rozšíření funkčnosti obsahuje další doplňkové moduly (pluginy).
2. Komunikace s WWW serverem – jedná se o vysílání požadavků na WWW server. Dále pak po přijetí dat ze serveru provádí dekódování dat a instrukcí (interpreter), sestavuje webovou stránku (rozložení prvků) a nakonec zobrazuje webovou stránku v okně (popř. přehrává další multimediální obsah).
3. Spolupráce s dalšími programy – spolupráce s dalšími programy pak závisí na dalších aplikacích nainstalovaných na zařízení, kde se nachází také prohlížeč. Jedná se např. o poštovní programy, editory atd.

Mezi nejpoužívanější WWW klienty v současné době patří Google Chrome (Google), Firefox (Mozilla Foundation), Internet Explorer (Microsoft), Safari (Apple Inc.), Opera, Opera Mobile (Opera Software ASA) a další. Jejich zastoupení na trhu se stále mění, často v závislosti na oblibě zařízení, která uživatelé pro využívání WWW služby používají. Např. v poslední době roste obliba mobilních zařízení (chytré telefony, tablety).

5.3.4 WWW SERVER

Webový server můžeme vnímat jak v podobě HW, tak v podobě SW. Má na starosti zpracovávání požadavků od WWW klientů a zasílání informací na základě těchto požadavků (např. zaslání webové stránky nebo souboru). Dále zasílá klientovi stavový kód odpovědi o tom, zda došla odpověď v pořádku nebo zda nastala chyba. Chybové odpovědi jsou pak číslovány dle typu chyby. Přijímané požadavky od klientů jsou protokolována a zpravidla ukládány do log souborů. Tyto log soubory jsou pak využívány při řešení problémů, v tom lepším případě pak bývají často zdrojem pro analýzu návštěvnosti webových stránek.Jako příklad webových serverů zde můžeme uvést např. Apache http server (Apache Software Foundtation), IIS (Microsoft), GWS (Google Web Server), nginx (NGINX, Inc.), a další. Mezi poměrně jednoduché servery patří například server Xitami. Mezi základní nastavení, které musíme u serverů provést, je definování uživatelů a skupin uživatelů, definování prostoru (disků, adresářů) pro umístění souborů a defaultní názvy souborů (stránek), které se zobrazí v případě, že se klient připojí k serveru a neuvede soubor pro zobrazení. Součástí www serverů bývá i propojení s databází (např. MySQL) a programovacím jazykem (např. PHP, Perl apod.). Většina www serverů současně funguje jako Ftp server.

SHRNUTÍ KAPITOLY

V této kapitole jste se seznámili se základy, principy a pravidly fungování Internetu