Střední odborná škola
a Střední odborné
učiliště Kuřim, s.r.o.

Úvod do počítačových sítí

Kuřim, říjen 2012 | Ing. Vojtěch Novotný

Obsah

1. Poskytování první pomoci

1.1 Postup při poskytování KPR

1. Zjistíme, zda není osoba v dosahu elektrického proudu, pokud ano, tak ji vyprostíme.
2. Zjistíme, zda je osoba v bezvědomí.
    - pokusíme se upoutat její pozornost hlasitým oslovením a zatřesením za rameno. Zběžně postiženého ohledáme, jestli nemá jiná život ohrožující poranění, která případně ošetříme
        - POKUD NEREAGUJE:
3. Zavoláme pomoc z okolí.
    - zavoláme hlasitým "Pomoc!" další zachránce z okolí
4. Zprůchodníme dýchací cesty.
    - pokud je to možné, zraněného uložíme na záda a dýchací cesty uvolníme prostým zakloněním hlavy a odstraněním překážek v dutině ústní (např. bahno u tonoucích, zvratky, ale i obyčejná žvýkačka nebo umělý chrup…)
5. Zjistíme, zda postižený dýchá.
    - přiložíme ucho k jeho ústům a kontrolujeme dýchání třemi smysly. Dech slyšíme, cítíme na tváři a vidíme, zda se zvedá hrudník
        - POZOR!, za zachovalé dýchání nepočítáme „lapavé“ dechy
        - POKUD NEDÝCHÁ:
6. Voláme 155.
    - uvedeme naše jméno, tel. číslo a polohu, zdravotní stav pacienta, případně povětrnostní podmínky a terénní přístupnost pro přistání vrtulníku lékařské záchranné služby.
7. Pokud zjistíme, že pacient:
    1. má zachované dýchání:
        - uložíme zraněného do stabilizované polohy a monitorujeme jeho životní funkce do příjezdu lékařské záchranné služby.
    2. nedýchá,
        - nezdržujeme se zjišťováním tepu, protože k zástavě krevního oběhu dochází v brzké době po zástavě dýchání

Pokud je v okolí AED (Automatizovaný externí defibrilátor) použijeme jej (necháme si jej přinést)

Zahájíme zevní srdeční masáž

1.2 Zevní srdeční masáž

- stlačujeme uprostřed hrudníku (dolní část hrudní kosti mezi prsními bradavkami)
- frekvence je 100 - 120 stlačení za minutu
- masírujeme s propnutýma rukama přeloženými zápěstími přes sebe (případně s propletenými prsty) kývavým pohybem celého těla
- stlačujeme do hloubky 5 cm, u dětí do hloubky 1/3 hrudníku
- při dvou zachráncích jeden poskytuje srdeční masáž, druhý plicní ventilaci, v případě únavy se mohou zachránci vystřídat po 2 minutách KPR

Obrázek 1. Masáž srdce

1.3 Plicní ventilace

- postiženému zakloníme hlavu
- prsty jedné ruky zacpeme nosní díry a nadechneme se (objem vdechu by měl být jako u normálního nádechu, velký objem vdechu je chybou!)
- široce otevřeme ústa, přitiskneme je kolem úst poraněného a vydechneme vzduch do jeho plic
- pozorujeme, jak se zvedá hrudník
- oddálením úst umožníme výdech, pozorujeme hrudník, zda klesá, a zároveň se nadechujeme

Obrázek 2. Dýchání z úst do úst

- máme-li k dispozici lékárničku, použijeme resuscitační roušku, nebo resuscitační masku

Shrnutí resuscitace			
	Poměr stlačení: vdechům	Rychlost – frekvence stlačení	Zahájení KPR
Dospělí	**30:2**	**100 - 120 stlačení za minutu**	30 stlačeními

1.4 Postiženého lze vyprostit z dosahu proudu

- vypnutím proudu (vypnout příslušný vypínač, vyšroubovat pojistky nebo vytáhnout zástrčku ze zásuvky)
- odsunutím vodiče nebo odtažením postiženého (suchým dřevem, suchým provazem, suchým oděvem, nikdy ne vlhkými nebo vodivými předměty. Nedotýkejte se holou rukou ani těla postiženého, ani vlhkých částí jeho oděvů. Pracujte pokud možno jen jednou rukou. Zajistěte postiženého, aby po přerušení proudu nespadl.)
- přerušením vodiče (např. přeseknutím sekerou se suchým topůrkem, izolačními kleštěmi apod.).

Video

Ukázka první pomoci - SZŠ Jaselská 2010 http://www.youtube.com/watch?v=XLnfjVzQNiI

Ukázky poskytování první pomoci od červeného kříže http://www.youtube.com/user/cckmost?feature=watch

Otázky, úkoly

- Co je nejdůležitější při poskytování první pomoci

Další zdroje ke studiu

- http://www.zzsvysocina.cz/index.php?page=1pomoc
- http://www.prvni-pomoc.webgarden.cz/

Použité zdroje

[1] Wikipedie: Otevřená encyklopedie: Kardiopulmonální resuscitace [online]. c2012 [citováno 30. 08. 2012]. Dostupný z WWW: <http://cs.wikipedia.org/w/index.php?title=Kardiopulmon%C3%A1ln%C3%AD_resuscitace&oldid=8352054>

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-09-01]. Dostupný pod licencí Public domain na WWW:
< http://cs.wikipedia.org/wiki/Soubor:CPR.jpg>

[2] Commons.wikimedia.org [online]. [cit. 2012-09-01]. Dostupný pod licencí Public domain na WWW:
< http://cs.wikipedia.org/wiki/Soubor:Insulfation2.jpg>

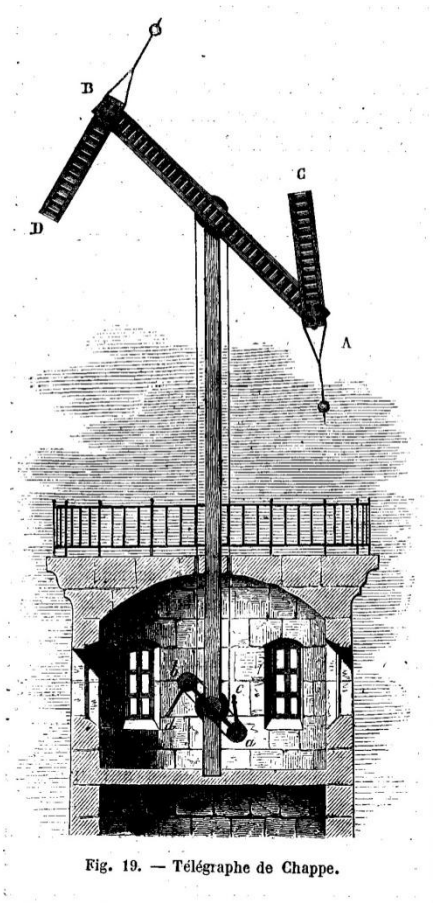
Úvod od počítačových sítí

2. Historie komunikace

Potřeba výměny různých informací a zpráv sahá hluboko do dějin lidstva. Se schopností řeči, přišla schopnost předávat informace. Nejprve ústním podáním, z člověka na člověka. Teprve později byly ty důležitější zaznamenávány písmem. Ve starém Sumeru, přibližně 4000 let před naším letopočtem, to byly hliněné destičky, do kterých člověk vyrýval své texty, které mohly být přenášeny pomocí poslů.

Již ve starověku se v některých specifických situacích lidé dokázali dorozumět pomocí optické signalizace – záblesky světla, vznikající odrazem od povrchu, který se alespoň zčásti choval jako zrcadlo, zapalováním strážních ohňů apod. Takto se pak lidé mohli například včas varovat před příchodem nepřítele.

Ucelenou organizací vynikala římská státní pošta (10 let př. n. l.), představovala vrchol tehdejšího systému v předávání zpráv a její dokonalá organizace zůstala na dlouhá staletí nepřekonána. Využívala sítě vynikajících silnic protínajících celou říši v neuvěřitelné délce celkových 100 000 kilometrů. Informace se šířily rychlostí koně.



Obrázek 3. Optický telegraf

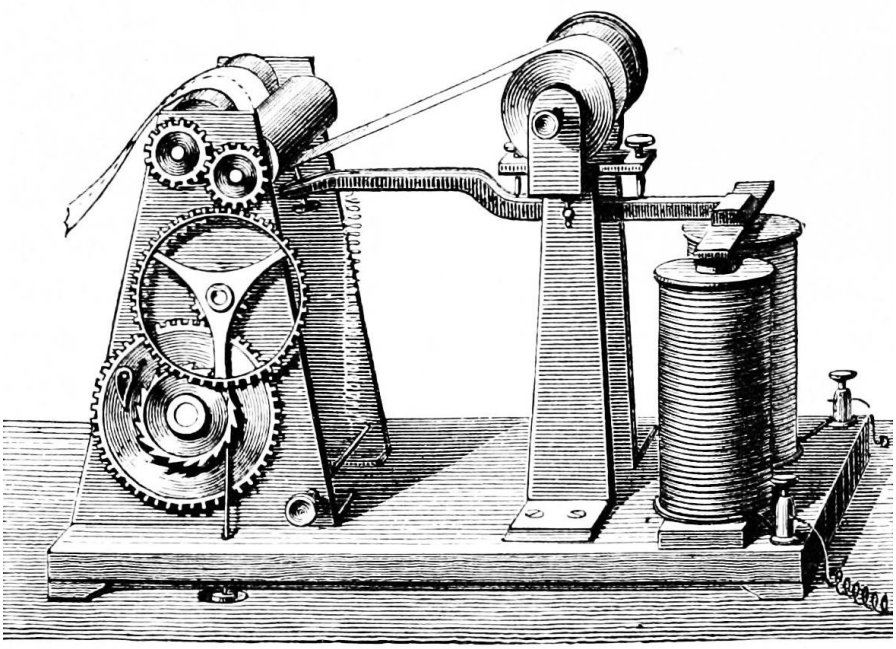
Optickým telegrafem propojili bratři Chappéové kolem roku 1793 Paříž s městem Lille (na vzdálenost asi 190 km a využívala cca 22 semaforových stanic), a umožnili přenos zpráv mezi těmito dvěma lokalitami v čase cca 5 minut. Vydržel až do roku 1852, kdy byl nahrazen telegrafem na elektrickém principu.

2.1 Telegraf

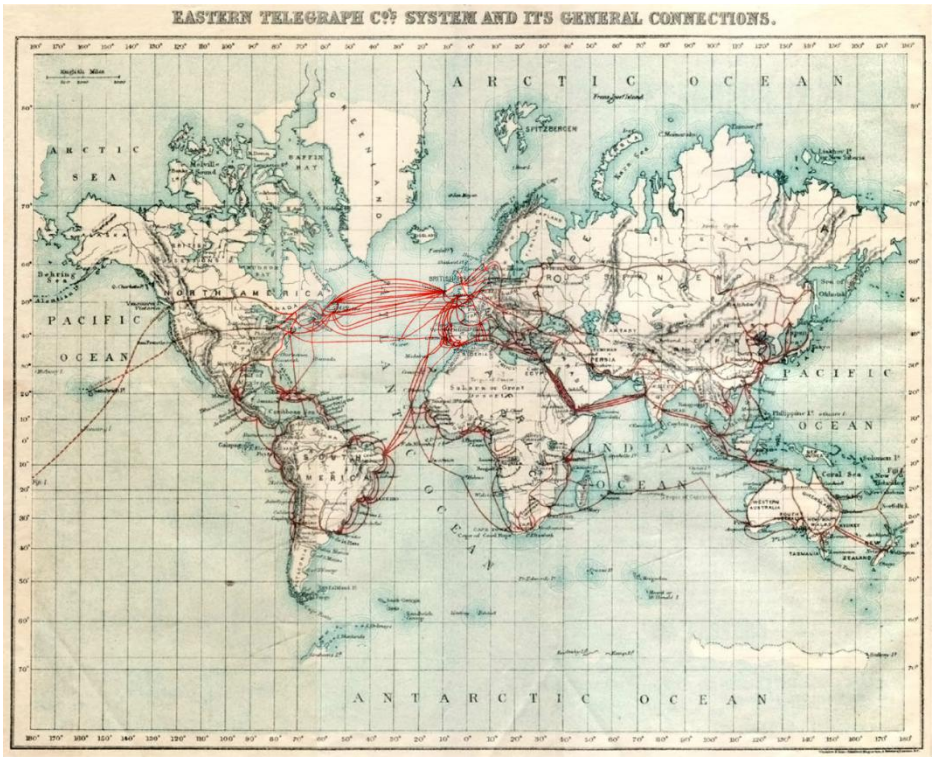
Za autora telegrafu je všeobecně považován pan Samuel Finlay Breese Morse byl totiž prvním, kdo svůj telegraf dovedl do stadia praktického použití: v roce 1844 vybudoval první telegrafní spojení mezi městy Baltimore a Washington (na vzdálenost cca 64 km), a v roce 1845 po této trase odvysílal první zprávu. Dosahoval přitom „úctyhodné“ přenosové rychlosti 2 bitů za sekundu.

Telegraf si pak již začal dobývat svět sám, a navíc dosti rychlým tempem.

V roce 1850 byly položeny první podmořské telegrafní kabely přes průliv La Manche. První mezikontinentální podoceánský kabelový spoj byl mezi Kanadou a Irskem zprovozněn na pouhých 26 dní v roce 1858 měděným vedením. Dosažená rychlost byla cca 25 slov za hodinu. Spoj byl obnoven v roce 1866, kdy byla rychlost již 8 slov za minutu. Spojení bylo komerční a jeho cena se pohybovala kolem 100 USD za 20 slov.



Obrázek 4. Morseův telegraf



Obrázek 5. Hlavní (podmořské) telegrafní trasy v roce 1901

2.2 Telefon

Rychlost, s jakou telegraf ovládl svět, byla vskutku impozantní. Příliš dlouho se ale tento vynález na výsluní také nehřál. Objevil se totiž jiný vynález, telefon, který rychle odsunul telegraf.

Za vynálezce telefonu je dnes všeobecně považován Alexander Graham Bell – rok 1876.

Na první transatlantický telefonní hovor si zájemci museli počkat, až do roku 1915, zatímco první telefonní rozhovor, přenášený přes družici, se mohl uskutečnit v roce 1962 (přes družici Telstar).

Obrázek 6. Družice Telestar II 1964

2.3 Bezdrátový přenos

V roce 1896 si fyzik Guglielmo Marchese Marconi v Londýně podává patent na bezdrátový telegraf. Již v roce 1901 podniká Marconi první úspěšné pokusy s přenosem rádiových vln přes Atlantik – v kanadském Newfoundlandu přijímá první zprávu ze starého kontinentu: tři tečky neboli písmeno S.

Za své rychlé rozšíření pak bezdrátové přenosy a radiotechnologie obecně vděčily dalším objevům (zejména pak objevu elektronky v roce 1904), díky kterým bylo možné konstruovat výkonné rádiové vysílače, a samozřejmě také dostatečně citlivé rádiové přijímače.

Obrázek 7. Terénní vysílačka 1955

Video

Princip optického telegrafu: http://youtu.be/qshGYE15u1A

Otázky, úkoly

- Zjistěte jaká je dnes přenosová rychlost páteřních telekomunikačních sítí.
- Jaké přenosové médium se dnes používá nejčastěji?
- Sestavte jednoduchý graf vyjadřující nárůst přenosové rychlosti komunikace v čase.

Další zdroje ke studiu

- Historie a budoucnost získávání informací http://iam.kryspin.net/2009/05/18/historie-komunikace-a-informaci/

Použité zdroje

[3] Historie poštovnictví. [online]. [cit. 2012-02-14]. Dostupné z: http://www.jablko.cz/Zajimavosti/Udalosti/Zajim_udalo_2.htm

[4] PETERKA, Jiří. *Z historie sdělovací techniky*. [online]. [cit. 2012-02-14]. Dostupné z: http://www.earchiv.cz/a94/a404c501.php3

Použité obrázky

[5] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW:
< http://commons.wikimedia.org/wiki/File:T%C3%A9l%C3%A9graphe_Chappe_1.jpg>

[6] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW:
http://commons.wikimedia.org/wiki/File:PSM_V03_D423_Morse_telegraph.jpg

[7] http://en.wikipedia.org/wiki/File:1901_Eastern_Telegraph_cables.png

[8] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW:
< http://commons.wikimedia.org/wiki/File:Telstar_II_Satellite_Parade_of_Progress.jpg>

[9] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW:
< http://commons.wikimedia.org/wiki/File:Bundesarchiv_Bild_183-29802-0001,_MTS_Strehla,_Bezirk_Dresden,_Ukw-Sprechfunk.jpg>

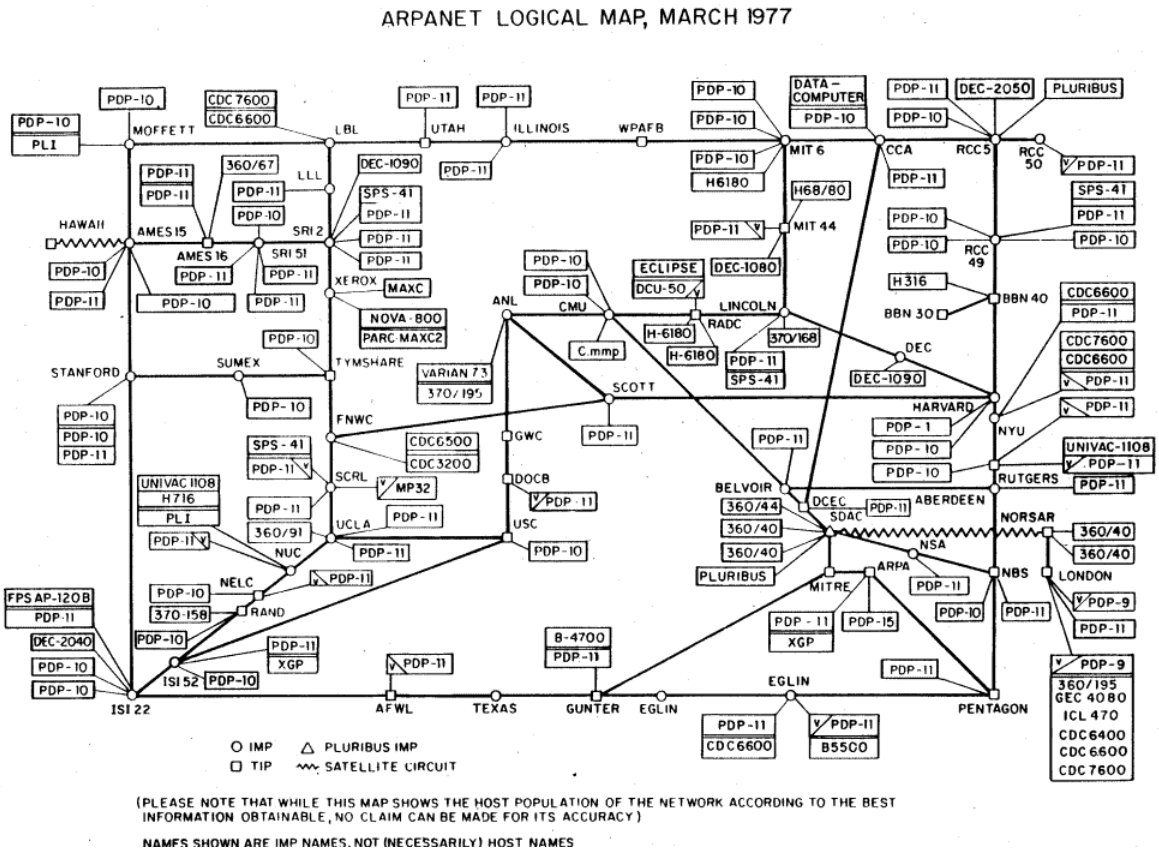
3. Vznik počítačových sítí

Počítačové sítě jsou sítě tvořené skupinou výpočetních systémů propojených přenosovými a spojovacími prostředky za účelem vzájemné komunikace.

S rozvojem třetí generace počítačů, počítačů s integrovanými obvody, se objevil požadavek umožnit mezi těmito počítači okamžitý přenos dat.

Stávající analogová telefonní síť nebyla vhodným prostředkem pro přenos dat mezi počítači, neboť byla navržena pro poskytování hovorových služeb a bylo třeba navrhnout nové řešení. Tak jako za mnoha dalšími technologiemi stál i za počítačovou sítí původně armádní výzkum.

- 1962 – vzniká projekt počítačového výzkumu agentury ARPA, což byla americká armádní agentura zabývající se vývojem technologií, které mají uplatnění ve vojenství.
- 1969 – vytvořena experimentální síť ARPANET, první pokusy s přepojováním uzlů (čtyři uzly). Armádní filosofie zapříčinila základní vlastnost - nezničitelnost - síť neměla žádné centrum, navíc spoje mezi jednotlivými uzly byly realizovány více cestami (odolnost proti výpadkům spojení)
- 1972 – ARPANET rozšířena na cca 20 směrovačů a 50 počítačů, použit protokol NCP (Network Control Program).

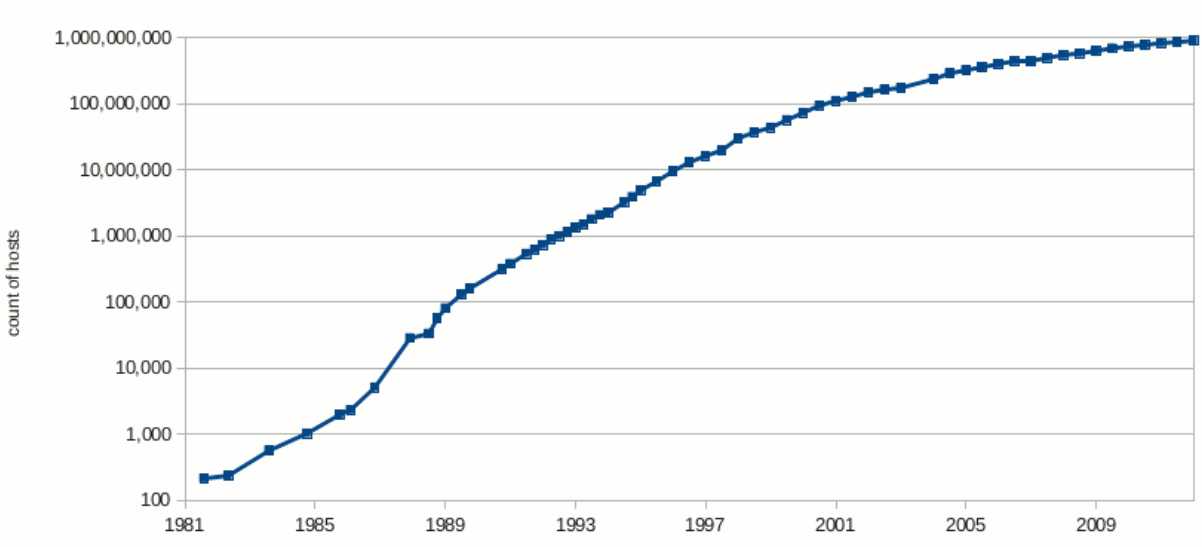


Obrázek 1. Stav ARPAnetu v roce 1977

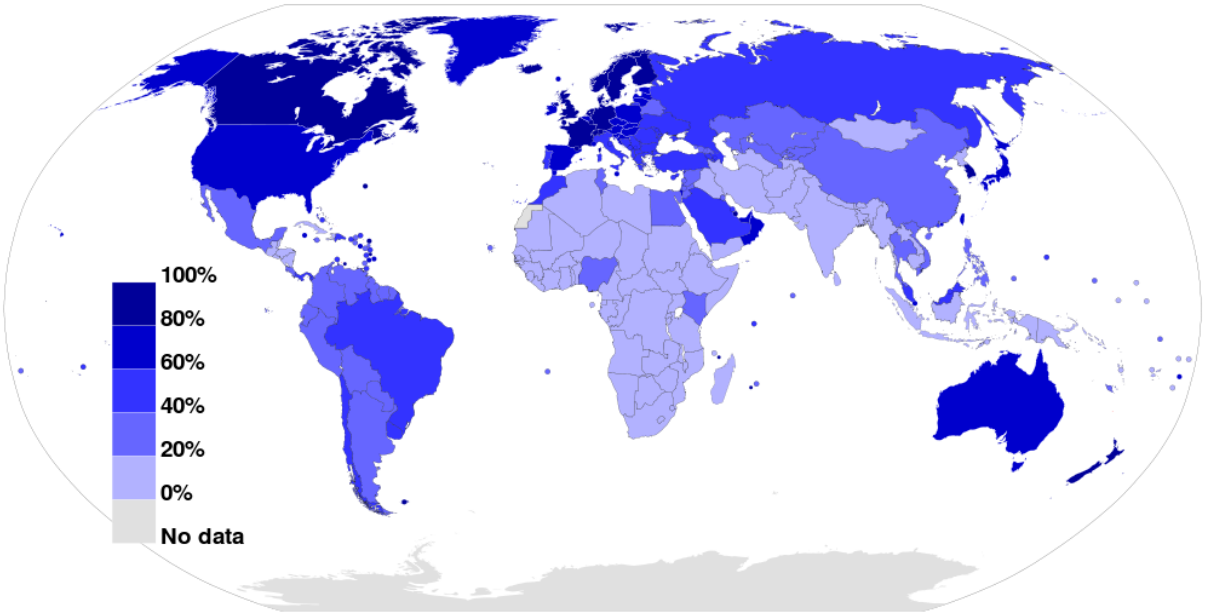
- 1972 – první e-mailový program.
- 1973 – byl navržen **paketový způsob komunikace**, tím byla zveřejněna idea vedoucí později k TCP/IP.
- 1980 – vznik protokolu IPv4, experimentální provoz TCP/IP v síti ARPANET.
- 1984 – vyvinut DNS (Domain Name System) – uživatel si nemusel pamatovat číselnou IP adresu, ale jen jednoduché doménové jméno. K ARPANETU připojeno pouhých 1000 počítačů.
- 1987 – vzniká pojem „Internet“. V síti je propojeno 27 000 počítačů.
- 1989 – Tim Berners-Lee v CERN v Ženevě publikuje návrh protokolu WWW (World Wide Web – propojení informačních zdrojů pomocí hypertextových odkazů), to je technologie webových stránek, kterou si dnes většina uživatelů představí pod pojmem Internet.

Obrázek 2. Počítač NeXT, který použil Tim Berners-Lee jako první Web server

- 1992 – připojen Bílý dům (vstup vládních institucí na Internet).
- 1993 – Mosaic, první WWW prohlížeč zdarma, který se celosvětově rozšířil.
- 1994 – vyvinut prohlížeč Netscape Navigator, Internet se komercionalizuje.
- 1996 – 55 milionů uživatelů, 2000 – 250 milionů uživatelů, 2003 – 600 milionů uživatelů, 2005 – 900 milionů uživatelů, 2010 – 1,8 miliardy uživatelů.



Obrázek 3. Nárůst počtu uživatelů Internetu 1981 - 2012. Všimněte si logaritmického měřítka.



Obrázek 4. Podíl obyvatel s přístupem k Internetu duben 2012

Uživatelé Internetu dle zemí		
	2006	2011
Afrika	3%	13%
Ameriky	39%	56%
Arabské Státy	11%	29%
Asie a Pacifické státy	11%	27%
Země commonwealthu	13%	48%
Evropa	50%	74%

Video

Historie počítačových sítí: http://youtu.be/7NpczzIsnLU

Otázky, úkoly

- Zjistěte, kolik má dnes Internet přibližné uživatelů. Kolik lidí vlastní mobilní telefon? Kolik lidí má přístup k pitné vodě?
- Kolik procent je to obyvatelstva.
- Sestavte jednoduchý graf vyjadřující nárůst počtu uživatelů Internetu v čase.
- Najděte na obrázku ARPANETu důležité americké instituce tehdejší doby.

Použité zdroje

[1] Internet. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2012 [cit. 2012-02-14]. Dostupné z: http://cs.wikipedia.org/wiki/Internet

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Arpanet_logical_map>

[2] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: <http://en.wikipedia.org/wiki/File:First_Web_Server.jpg>

[3] Commons.wikimedia.org [online]. [cit. 2012-08-14]. Dostupný pod licencí Creative Commons na WWW: < http://en.wikipedia.org/wiki/File:Internet_host_count_1988-2012_log_scale.png>

[4] Commons.wikimedia.org [online]. [cit. 2012-08-14]. Dostupný pod licencí Creative Commons na WWW: < http://commons.wikimedia.org/wiki/File:InternetPenetrationWorldMap.svg>

4. Důsledky existence počítačových sítí

4.1 Přínosy počítačových sítí

- komunikační prostředek – zjednodušení a zrychlení komunikace mezi lidmi (e-mail, instant messaging služby, postupná integrace různých komunikačních služeb do počítačových sítí – IP telefonie (VoIP), videotelefonie, atd.),
- elektronická forma přenosu dat mezi počítačovými systémy,
- sdílení výpočetní a paměťové kapacity,
- sdílení drahých periférií – tiskárny,
- centrální řízení procesů,
- přístup k rozsáhlým informačním zdrojům,
- centralizace a zjednodušení správy počítačových systémů – mnoho úprav a změn lze provádět vzdáleně,
- centrální dohled nad monitorovanými objekty,
- prostředek vzdělávání,
- prostředek zábavy,
- vzdálená spolupráce při řešení úkolů,
- prostředek pro reklamu výrobků a služeb,
- elektronické obchodování – elektronické obchody,
- elektronické bankovní služby,
- cloud computing – na Internetu založený model vývoje a používaní počítačových technologií, poskytování služeb či programů uložených na serverech na Internetu,
- zvýšení spolehlivosti systémů a bezpečnosti dat (clustery),…

4.2 Negativní důsledky počítačových sítí

- prostředek pro provozování nelegálních aktivit,
- porušování autorských práv,
- rychlé šíření počítačových virů,
- nebezpečí útoků na systémy a spravovaná data,
- možnost odposlouchávání či pozměnění přenášené informace,
- možnost šíření nepravdivých či poplašných zpráv (hoax),
- možnost šíření nevyžádané reklamy (spamming),
- změna psychiky a komunikativních schopností lidí,…

4.3 Ochrana soukromí

- přímé hrozby

- spyware – sleduje uživatelovy aktivity, zjišťuje využitelné (zneužitelné) informace
- phishing – podvodné předstírání reálné služby (např. „aktualizace uživatelských účtů v bance) na falešném serveru s cílem získat přístup (heslo) ke službě (internetové bankovnictví)

- potenciální hrozby

- často se pod jednou střechou nabízí řada služeb zdarma (např. Google: pošta, kalendář, dokumenty, fotografie, RSS čtečka, mapy,... Facebook,…); poskytovatel získává informace o uživatelích.

Otázky, úkoly

- Co je dnes hlavním motivem pro tvůrce virů?
- Podle čeho lze identifikovat hoax?
- Zamysli se nad tím, jaký by byl týden bez internetu pro tebe.
- Zamysli se nad tím, jaký by byl týden bez internetu pro celý svět.
- Najdi další důvody existence počítačových sítí.

5. Netiketa

Netiketa je jakási pomyslná sbírka pravidel a zásad, která by se měla dodržovat v internetovém světě.

Mnoho lidí si myslí, že při vstupu do internetového světa mají naprostou anonymitu. Což je velký omyl – téměř vždycky se dá pomocí různých metod internetový uživatel vystopovat. Většina uživatelů si to neuvědomuje, takže opakovaně vstupuje do nebezpečí tím, že na sociálních sítích, chatech nebo diskuzích ostatní uživatele urážejí, vysmívají se jim nebo se o nich vyjadřují vulgárně.

Je třeba si uvědomit, že v internetovém světě bychom se měli chovat podobně jako ve světě reálném, to je jako civilizovaní lidé. Za tím účelem existuje netiketa, pravidla slušného chování na Internetu.

5.1 Pravidla

- Nezapomínejte, že na druhém konci jsou lidé a ne počítač. To, co napíšete do počítače, byste možná dotyčnému nikdy neřekli do očí.
- Dodržujte obvyklá pravidla slušnosti normálního života. Co je nevhodné v obvyklém životě, je samozřejmě nevhodné i na internetu.
- Zjistěte si taktně, s kým mluvíte. Internet je přístupný lidem z celého světa, a v každé zemi platí jiná morálka. Co je dovolené na americkém chatu, nemusí být dovolené na arabském, a to platí o všech podobných skupinách. Politika, náboženství a podobné problémy by proto měly být diskutovány s maximálním taktem a v mezích slušnosti.
- Berte ohled na druhé. Neposílejte proto zbytečně velké e-mailové zprávy.
- Je vhodné psát s diakritikou. Vyvarujete se tak nedorozumění. Nekomolíte rodnou řeč. Pokud jste z nějakého důvodu nuceni psát bez diakritiky, snažte se používat správný pravopis.
- Nezveřejňujte nepravdivé, nebo i pravdivé, ale choulostivé informace.
- Pomáhejte v diskuzích. Pokud má někdo v diskuzi nějaký problém, odpovězte mu, pokud znáte odpověď. Někdo jiný zase pomůže vám. Platí zásada: „Napřed poslouchej, pak piš.“
- Respektujte soukromí jiných. Pokud vám omylem přišla zpráva, která vám nepatří, je vhodné ji smazat a taktně upozornit odesilatele na jeho chybu.
- Nezneužívejte svou moc či své vědomosti. Pokud jste správce serveru, máte sice přístup k poště ostatních, ale nemusíte ji kontrolovat jenom tak z nudy.
- Odpouštějte ostatním chyby. I vy je děláte. Nevysmívejte, a nenadávejte jim.

- Nešiřte hoaxy (poplašné či falešné zprávy). Zahlcují internet. Pokud vám přijde hoax, zdvořile upozorněte odesilatele, že takové jednání je nevhodné.
- Nerozesílejte spam a reklamu. Neporušujte autorská práva.

Otázky, úkoly

- Proč je snadnější říkat a dělat špatné věci na „přes Internet“?
- Zažili jste „internetovou šikanu“? Jak se proti ní bránit?

Další zdroje ke studiu

- Pravidla slušného chování na internetu http://www.emag.cz/netiketa/

Použité zdroje

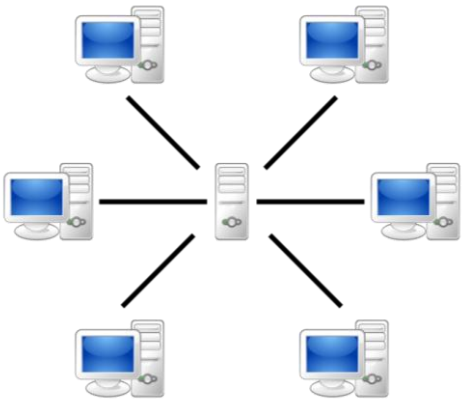
[1] Netiketa. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2012 [cit. 2012-02-14]. Dostupné z: <http://cs.wikipedia.org/wiki/Netiketa>.

6. Vlastnosti počítačových sítí

6.1 Vztahy mezi uzly (procesy) v síti

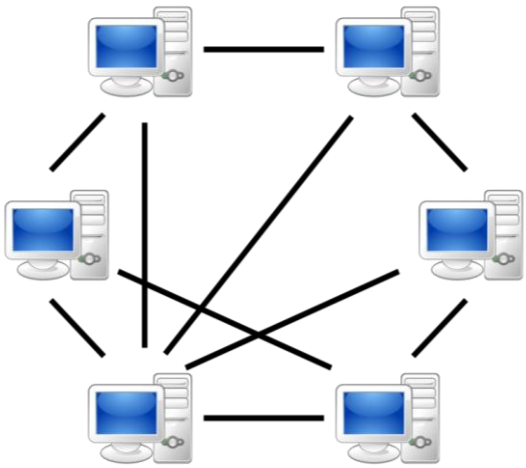
terminál-hostitelský počítač – terminál (či proces) je pouhým prodloužením přípojných kabelů monitoru, klávesnice a případně ovládacího prvku (myš, dotyková ploška, apod.) přes síť. Zadávané příkazy z terminálu jsou vykonávány procesy běžícími na hostitelském počítači a výsledky jsou posílány na terminál.

klient-server – software realizující danou síťovou službu je rozdělen do dvou částí, klienta a serveru. Klient posílá požadavky a zobrazuje výsledky a server přijímá příkazy, kontroluje, zda je možno příkaz vykonat (správná syntaxe, patřičná oprávnění, atd.), vykonává příkaz a zasílá klientské části výsledky operace. Jedná se o nejčastější případ v internetu.



Obrázek 1. Model klient-server

peer-to-peer (P2P) – komunikující aplikace jsou si rovnocenné, tzn., že daná aplikace žádá od protějšku služby a také je sama poskytuje.



Obrázek 2. Model peer-to-peer

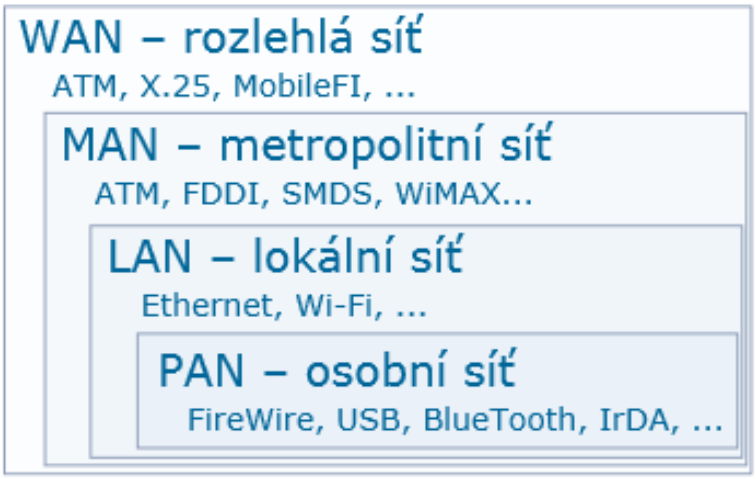
6.2 Typy počítačových sítí podle rozsahu

PAN (Personal Area Network / Pico Area Network) – je počítačová síť tvořená komunikujícími zařízeními jako mobilní telefon, PDA nebo laptop, které jsou v blízkosti jedné osoby. Dosah takové osobní sítě je většinou jen několik metrů. Používá se ke komunikaci mezi samotnými zařízeními nebo k připojení k okolním sítím nebo k Internetu. PAN mohou být drátové (například přes USB nebo FireWire) i bezdrátové (například pomocí IrDA nebo Bluetooth).

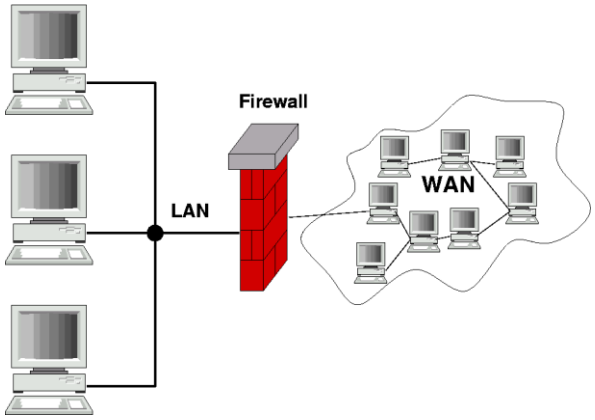
LAN (Local Area Network) – lokální počítačové sítě s vysokou přenosovou rychlostí a propustností, pro propojení počítačů v rámci jedné či několika budov, se sdílením přenosové kapacity, s dosahem řádově stovky metrů až jednotky kilometrů, ve vlastnictví jedné organizace, koncové uzly lze vypínat bez ohrožení chodu zbytku sítě.

MAN (Metropolitan Area Network) – metropolitní (městské) sítě, s relativně vysokou přenosovou rychlostí, avšak nižší propustností, s dosahem řádově desítky kilometrů, ve vlastnictví síťových operátorů, s nepřetržitým provozem síťových uzlů.

WAN (Wide Area Network) – sítě často s nižší přenosovou rychlostí (až na vysokorychlostní optické páteře), avšak s ještě nižší propustností, s dosahem řádově stovky až tisíce kilometrů, ve vlastnictví jednoho i více síťových operátorů, s nepřetržitým provozem síťových uzlů.



Obrázek 3. Dělení sítí dle rozlehlosti



Obrázek 4. Obecný příklad napojení LAN do WAN

Otázky, úkoly

- Zjistěte jaké technologie (protokoly) reprezentují PAN, LAN, MAN a WAN.
- Jakým způsobem se dnes používá terminálové připojení.
- Vyzkoušej si terminálové připojení.
- Kdo vlastní a provozuje WAN sít Internet?

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: <http://en.wikipedia.org/wiki/File:Server-based-network.svg>

[2] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: <http://en.wikipedia.org/wiki/File:P2P-network.svg>

[3] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: < http://commons.wikimedia.org/wiki/File:DruhyPocitacovychSiti.svg>

[4] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: <http://cs.wikipedia.org/wiki/Soubor:Gateway_firewall.png>

7. Struktura sítí LAN

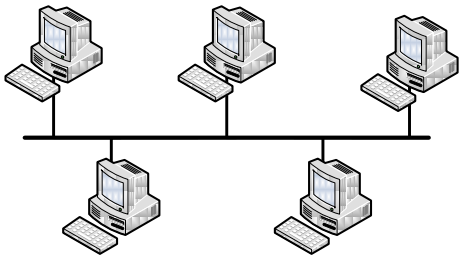
Propojené uzly sítě mohou vytvářet různé konfigurace, které jsou určeny typem dané sítě, přičemž struktura závisí na úrovni pohledu

- **fyzická** – jakou konfiguraci vytváří fyzické propojení počítačů,
- **vizuální** – jakou topologii síť vytváří z vizuálního hlediska,
- **logická** – jakou konfiguraci síť tvoří z pohledu linkové vrstvy (lépe řečeno z pohledu MAC podvrstvy – jakým způsobem jsou posílány rámce).

Sítě tvoří následující struktury:

sběrnice – stanice (uzly) sdílí fyzicky či logicky jeden přenosový kanál v každém směru. Stanice jsou k fyzické sběrnici (např. koaxiální kabel) připojeny vysokoimpednačně, takže vypnutí či výpadek stanice zpravidla neohrozí činnost sítě. Síť nepotřebuje centrální prvek.

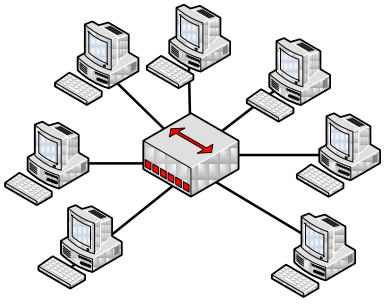
- Výhody: Není nutnost centrálního prvku.
- Nevýhody: Přerušení sběrnice znemožní kompletně komunikaci.



Obrázek 1. Topologie sběrnice

hvězda – koncové stanice jsou propojeny přes centrální uzel, který je všemocným a pro chod sítě nejdůležitějším prvkem v síti. Funkčnost a bezchybná činnost centrálního uzlu je nezbytným předpokladem činnosti sítě.

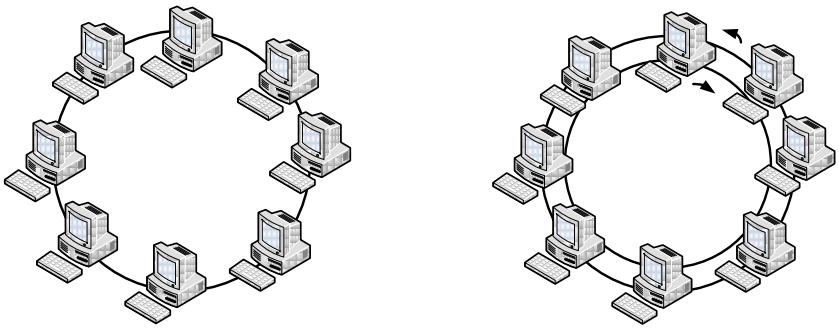
- Výhody: Přerušení jakékoliv linky znemožní komunikaci jen k danému uzlu.
- Nevýhody: Nutnost centrálního prvku. Větší množství kabelů.



Obrázek 2. Topologie hvězda

kruh – stanice jsou uspořádány do fyzického či logického kruhu, čímž je určena posloupnost přidělování práv k přístupu ke sdílenému médiu. Musí být vyřešena problematika odstoupení a přihlášení se stanice do sítě.

- Výhody: Není nutnost centrálního prvku. Lehká implementace priorit. Jednoduché protokoly.
- Nevýhody: Přerušení sběrnice znemožní kompletně komunikaci. Nepružné – hůře se přidávají další uzly.



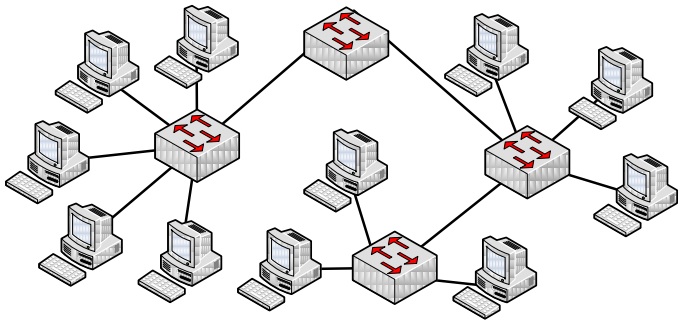
Obrázek 3. Topologie kruh a dvojitý kruh

Kruh může být:

- jednoduchý – narušení kruhu způsobí ukončení činnosti sítě,
- dvojitý – druhý kruh může být využit pro
  - zálohu v případě výpadku primárního kruhu,
  - opačný směr přenosu (download/upload).

strom – propojení počítačů tvoří stromovou hierarchickou strukturu. Typickým příkladem je síť Ethernet na bázi přepínačů. Strom je vlastně několik hvězd spojených dohromady, tak aby byla splněna postupná hierarchie.

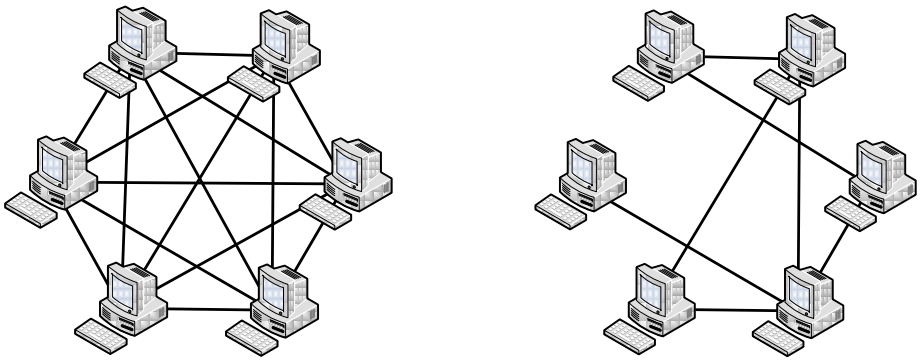
- Výhody: Přerušení jakékoliv linky znemožní komunikaci k danému uzlu nebo rozpad stromu na části, které ovšem mohou zůstat funkční. Vysoce modulární struktura.
- Nevýhody: Nutnost centrálních prvků. Neexistuje „záložní cesta“.



Obrázek 4. Topologie strom

polygon – uzly sítě jsou navzájem propojeny tak, že mezi dvěma body existuje zpravidla více cest. Je to výhodné pro vyšší bezpečnost doručení dat. Tato architektura se používá tam, kde to princip přenosu datových jednotek umožňuje, a to nejčastěji na úrovni propojení směrovačů. Při úplném polygonu prudce narůstá celkový počet cest v síti. Máme-li n uzlů je celkový počet cest = $\frac{n(n-1)}{2}$.

- Výhody: Přerušení jakékoliv linky zpravidla existuje jiná cesta. Vysoce modulární struktura.
- Nevýhody: Úplný polygon je topologie spíše teoretická, protože při narůstajícím počtu uzlu prudce narůstá nutný počet cest. Při neúplném polygonu jsou větší nároky na aktivní prvky – musí hledat cestu.



Obrázek 5. Topologie úplný polygon a obecná topologie (neúplný polygon)

Otázky, úkoly

- Jakou topologii používáte doma?
- Jaká topologie se používá ve škole?
- Jaká topologie se používá pro Internet?

- Zjisti, proč u topologie strom nemohou existovat mezi dvěma uzly dvě cesty.

Další zdroje ke studiu

Použité obrázky

[1] Autorem obrázků je Vojtěch Novotný.

Přístup k přenosovému médiu

Signál nesoucí informaci se přenáší určitým komunikačním kanálem, který musí být v okamžiku vysílání volný, aby nedocházelo k znehodnocení vyslané informace. Často se totiž stává, že daná přenosová kapacita spoje je využívána pro mnoho přenosů. Musí být tedy implementovány metody, které řeší problematiku sdílení přenosové kapacity. Metody lze v nejhrubším pohledu rozdělit na statické a dynamické.

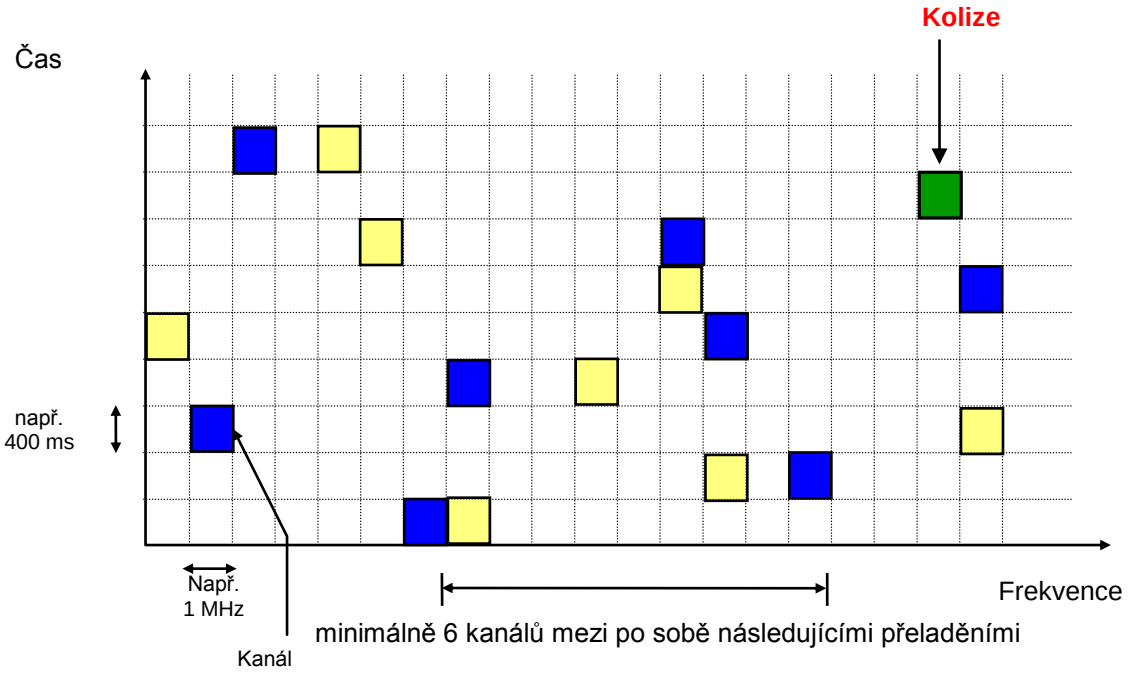
8. Statické přístupové metody

Princip statických přístupových metod spočívá v tom, že danému přenosu je po celou dobu komunikace (komutované spoje) či dokonce stále (pevné spoje) vyhrazena určitá přenosová kapacita. Výhodný je v situaci, kdy jednotlivé vstupy generují rovnoměrné datové toky, bez významnějších odchylek v čase. Pak má smysl a je efektivní rozdělit celkovou přenosovou kapacitu na příslušný počet částí, a toto rozdělení dále neměnit.

Existuje řada způsobů:

- **prostorové dělení - SD** (Space Division) - každý spoj je řešen zvláštním vedením. Mezi každými dvěma účastníky existuje přímé spojení. U bezdrátových spojů je pastorové dělení řešeno dostatečnou vzdáleností v prostoru nebo použitím úzce směrových antén, tak aby se jednotliví účastníci při komunikaci neovlivňovali.
- **kmitočtový multiplex - FDMA** (Frequency Division Multiple Access) - každé spojení je realizováno v jiném kmitočtovém pásmu. V praxi je ovšem FDMA nevýhodný kvůli tomu, že jde o analogovu techniku - různé frekvenční posuny, vzájemné slučování a následné oddělování nejsou nikdy ideální, a vždy určitým způsobem znehodnocují přenášený signál. Typické použití je např. u rozhlasových stanic.
- **časový multiplex - TDMA** (Time Division Multiple Access) - signál je sdružen se signály ostatních spojů do jednoho vysokorychlostního spoje. Vzniká tak virtuální rámec, kde každému spoji je přidělen určitý časový slot - timeslot. Uzel odvysílá svoji zprávu v určeném timeslotu a pak musí čekat, než na něj dojde opět řada. Rozdělení ovšem nemusí být rovnoměrné, ale mělo by být neměnné v čase.
- **kódový multiplex - CDMA** (Code Division Multiple Access) - přenos s rozprostřeným spektrem, kdy každému spoji je přidělena určitá posloupnost, která řídí způsob vysílání. Každý vysílač svá data nejprve vhodně zakóduje pomocí dané posloupnosti, a pak rovnou vysílá, na stejné frekvenci a ve

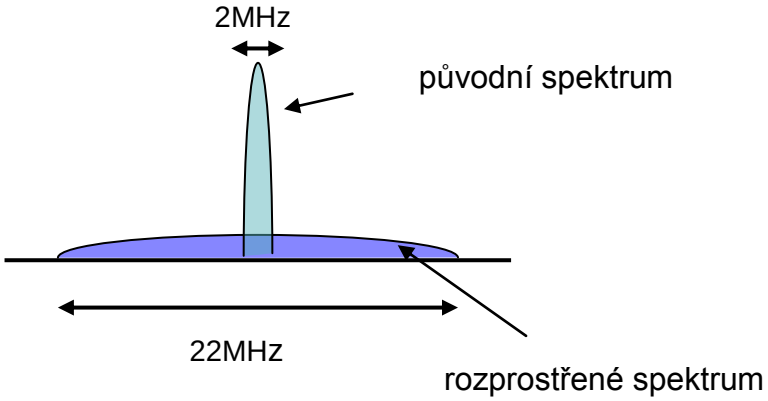
stejném čase jako ostatní vysílače. V éteru pak dochází ke smíchání všech signálů. Důležité je, že každý přijímač je schopen z přijaté směsi „vytáhnout“ právě to, co vyslal vysílač, jehož data chce přijímat. Toho dosáhne tím, že zná kódování vysílače a ví tedy, kde přijaté směsi hledat vyslaná data. CDMA je moderní statická přístupová metoda umožňující dosahovat vyšších přenosových rychlostí. Je šetrná k přenosovému spektru a odolná proti rušení.



Obrázek 1. Kmitočtové skákání - příklad koexistence 2 sítí (žlutá a modrá) v jedné podmnožině kanálů

Každý datový bit je kódován jako 11 bitů (tzv. čipů).

Tím se 11krát zvyšuje přenosová rychlost a zároveň i rozprostírá vysílaný výkon do 11krát širšího pásma a 11krát se snižuje výkonová hustota signálu.



Obrázek 2. Rozprostření spektra

Řada aplikací využívá kombinace několika výše uvedených metod. Například systém GSM pracuje na bázi kombinace FDMA, SD a TDMA.

Otázky, úkoly

- Jakým způsobem kombinuje GSM přístupové metody?
- V čem jsou statické přístupové metody nevýhodné?
- Kódový multiplex dokáže svoje vysílání skrýt tak, aby nebylo odhalitelné, jak to dělá?

Další zdroje ke studiu

- Báječný svět počítačových sítí, část VII. - Přenosové techniky http://www.earchiv.cz/b05/b1000001.php3

Použité obrázky

[1] Autor Vojtěch Novotný

[2] Autor Vojtěch Novotný

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

[2] BURDA, Karel, doc. Ing. CSc. *Návrh, správa a bezpečnost počítačových sítí*. FEKT VUT v Brně, Brno 2007.

9. Dynamické přístupové metody

Oproti statickým je u dynamických metod celá přenosová kapacita k dispozici všem přenosům a jednotlivé zdroje se musí o přidělení možnosti vysílat určitým způsobem ucházet – často i soupeřit.

Přístup se řeší implementací frontových a případně prioritních mechanizmů nebo na principu náhodného přístupu, který ovšem nedovoluje zavedení priorit.

Dynamické přístupové metody a lze rozdělit do několika skupin:

9.1 deterministické – s centrálním přidělováním

metody garantují maximální zdržení, než se stanice dostane k vysílání a umožňují implementaci priorit

- **s centrálním přidělováním** – v síti existuje centrální uzel, který uděluje koncovým stanicím oprávnění k vysílání a to:
  - **na žádost** – koncová stanice žádá centrální uzel o právo vysílat,
  - **na výzvu** – centrální stanice se dotazuje koncových stanic, zda nechtějí vysílat.

9.2 distribuované

- **fyzický kruh** – stanice spojené do fyzického kruhu si mezi sebou po směru vysílání předávají pověřovací rámec, kterým se stanici, která tento rámce obdrží, na určitou dobu pronajímá přenosová kapacita kruhu (např. Token Ring).
- **logický kruh** – stanice jsou fyzicky spojeny do jiné topologie (sběrnice, hvězda), avšak z hlediska řízení přístupu tvoří logický kruh, kdy si stanice opět předávají pověření opravňující přístup ke sdílenému přenosovému kanálu.

9.3 náhodné

přístup ke sdílenému kanálu je náhodný proces. Není zaručeno, kdy se stanice dostane k možnosti odeslat zprávu.

- **Aloha** – koncová stanice zahájí vysílání v kterýkoliv okamžik, aniž by si ověřila, zda již nevysílá jiná stanice a zda její data nebyla znehodnocena vysíláním jiné stanice. Tato metoda vykazuje velmi nízké procento reálné propustnosti z celkové kapacity kanálu asi (při více stanicích asi jen 20 %).
- **Slotted Aloha** – koncová stanice může zahájit vysílání pouze v pevně stanovených okamžicích (čas je rozdělen do slotů). Maximální dosažitelné využití kapacity se tak téměř zdvojnásobí (35%).

- **CSMA (Carrier Sense Multiple Access)** – koncová stanice před vlastním vysíláním kontroluje obsazení kanálu. Pokud je kanál obsazený, stanice čeká a pravidelně kontroluje jeho stav. Je-li volný, pak záleží na podptypu metody.

  CSMA (naléhající), Po uvolnění kanálu začne okamžitě vysílat. Pokud dojde ke kolizi s vysíláním jiné stanice, odloží opakované vysílání na náhodně zvolenou pozdější dobu. Využitelná kapacita komunikačního kanálu, je nyní asi 45%.

  CSMA (nenaléhající), se označuje také jako CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Stanice vyčká určitou náhodnou dobu a teprve pak, je-li kanál ještě volný, se začne vysílat. Bylo zjištěno, že k zahlcení sítě nedochází, ale odezva systému na požadavek vysílání je příliš dlouhá.

  CSMA (*p*-naléhající), je kompromisem mezi dvěma výše uvedenými metodami. S pravděpodobností p se chová jako naléhající, s pravděpodobností 1 – p jako nenaléhající CSMA. Při *p* kolem 5% je výsledek optimální – doba odezvy systému je malá a přitom nedochází k zahlcení.

- **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)** – metoda se používá u sítě Ethernet a jedná se o naléhající metodu CSMA avšak s detekcí kolizí (to není u bezdrátových sítí možné).

algoritmus CSMA/CD:

- 1. pokud má stanice k vyslání blok dat (tzv. rámec), tak zkontroluje, zda nějaká stanice nevysílá po dobu kolizního slotu (ten je dán rychlostí sítě a minimální délkou rámce, např. pro 10 Mb/s a 512 bitů je doba 51,2 μs).
- 2. Pokud nikdo nevysílá, tak okamžitě zahajuje vysílání. Pokud někdo vysílá, čeká na konec tohoto vysílání. Okamžitě poté začne vysílat.
- 3. V průběhu vysílání porovnává signál, co vysílá se signálem co je ve skutečnosti na přenosovém médiu. Když v průběhu vysílání zjistí cizí signál ve svém přijímači, tak nastala kolize. Stanice, která detekovala kolizi první, přeruší vysílání, vyšle speciální sekvenci bitů (tzv. JAM) a náhodně si určí okamžik dalšího pokusu o vysílání (tj. návrat na bod 1).
- Maximálně 16 pokusů o vysílání, pak ohlásí neúspěch.

Nevýhodou této metody je, že nezaručuje maximální dobu, za jakou se stanice dostane k úspěšnému odeslání rámce. Využití sítě nejdříve narůstá se zátěží. Se zvyšováním zatížení sítě se však kolize stávají stále častějšími a nárůst využití sítě se zvolňuje, až po překročení určité zátěže začne pozvolna klesat.

Otázky, úkoly

- Používá Ethernet stále CSMA/CD?
- V čem jsou dynamické přístupové metody nevýhodné?
- Proč je metoda Aloha tak málo účinná?

Další zdroje ke studiu

- Báječný svět počítačových sítí, část VII. - Přenosové techniky http://www.earchiv.cz/b06/b0100001.php3

Použité obrázky

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

10. Modulace

10.1 Přenos dat

Potřebujeme-li přenášet dvojková data po signálových vodičích, můžeme obě možné hodnoty, 0 a 1, reprezentovat pomocí úrovní napětí na vodiči jednou nulovou a jednou nenulovou úrovní, či jednou zápornou a jednou nezápornou úrovní. Používají se ovšem i složitější způsoby vyjádření logických hodnot pomocí úrovní napětí. Všechny tyto způsoby přenosu jsou souhrnně označovány jako přenosy v základním pásmu.

Problém je však v tom, že mnohé přenosové cesty (např. běžné telefonní okruhy apod.) jsou vzhledem ke svým fyzikálním vlastnostem pro přenos v základním pásmu prakticky nepoužitelné.

Alternativou k přenosu v základním pásmu je přenos v přeloženém pásmu, při kterém je přenášen takový signál, který se daným přenosovým médiem šíří nejlépe (s nejmenšími ztrátami). Typicky jde o pravidelně se měnící signál sinusového průběhu (tzv. harmonický signál). Užitečná informace se pak přenáší prostřednictvím změn v průběhu tohoto signálu. Lze si představit, že harmonický signál je jakýmsi nosičem (proto se mu také říká nosný signál resp. nosná, anglicky carrier) a užitečná informace se na něj "nanáší" postupem označovaným jako modulace.

10.2 Amplitudová modulace (ASK)

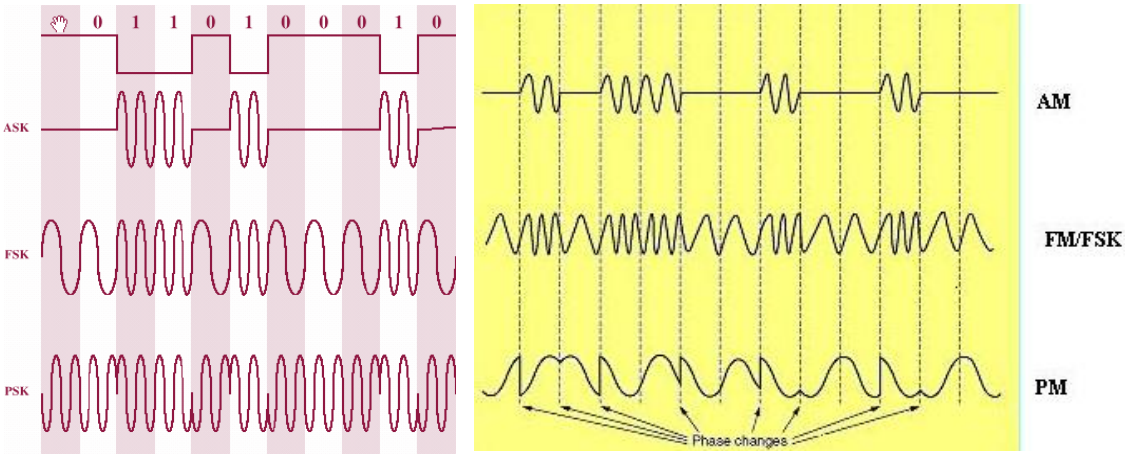
V závislosti na změně modulačního signálu se mění amplituda nosného signálu. Frekvence ani fáze nosné vlny se u této modulace nemění. Historicky je to nejstarší druh modulace. Je také nejjednodušší. Začala se používat při experimentech s radiovým vysíláním těsně po roce 1900. V běžném prostředí je málo odolná proti rušení. V dnešní době je však vhodná pro přenosy optickými vlákny (paprsek svítí 1 x paprsek nesvítí 0).

10.3 Frekvenční modulace (FSK)

Frekvence nosné funkce je rozkmitávána ze své polohy úměrně informačnímu signálu. Dvě binární hodnoty jsou reprezentovány dvěma různými frekvencemi v blízkosti nosné. Informace je tedy kódována nikoliv změnou amplitudy nebo fáze, ale změnou frekvence nosné vlny. Odolnost proti chybám je lepší než u ASK.

10.4 Fázová modulace (PSK)

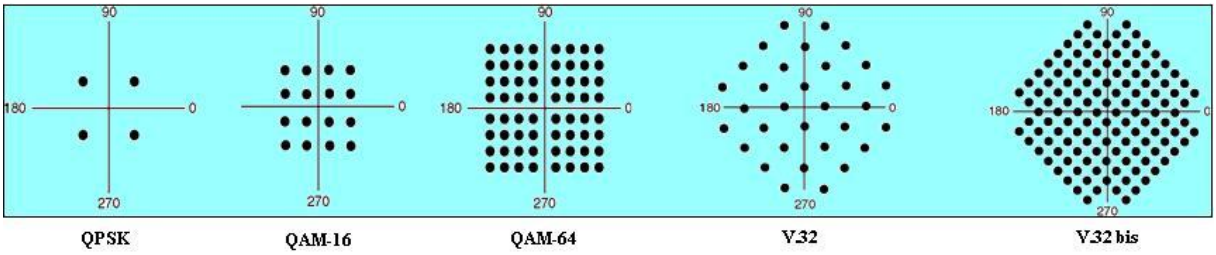
Fáze osciluje kolem klidové polohy, většinou kolem nulového fázového úhlu, a např. při modulaci hodnoty 1 dojde vždy k posunutí fáze o 180°. Změna fáze je vyhodnocována oproti předchozímu intervalu. Je odolná proti rušení.



Obrázek 1. Časové průběhy modulovaných signálů ASK, FSK, PSK

10.5 Další modulace

Existuje a dnes se převážně používá celá řada dalších složitějších modulací vznikajících hlavně kombinací výše uvedených metod.



Obrázek 2. Diagramy složitějších modulací.

Otázky, úkoly

- Jaké modulace používá rádio?
- Najdi příklad další modulace.
- Namaluj, jak by se použilo ASK, FSK a PSK při vícestavové modulaci?

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: <http://en.wikibooks.org/wiki/File:1a23.jpg>

[2] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: < http://en.wikibooks.org/wiki/File:Mple.jpg>

11. Přenosové médium

Charakteristiky médií:

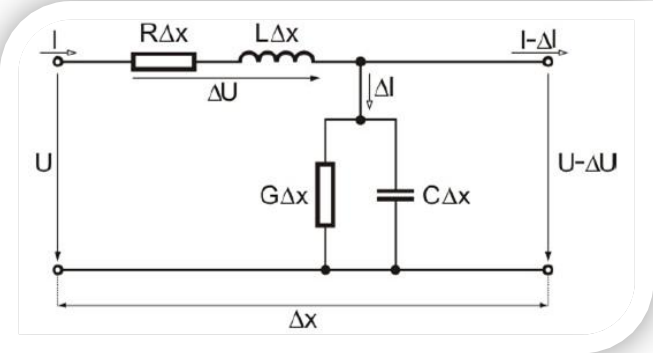
- **Útlum** je dán zmenšením výkonu signálu. Udává se v dB. Rozeznáváme útlum napětí, proudu a výkonu. Např. útlum výkonu se vypočítá:

$$P = 10\log\frac{\text{vstupní výkon}}{\text{výtupní výkon}}\ [dB]$$

V tomto případě útlum o 3 dB znamená jeho snížení na polovinu.

- **Zkreslení** – deformace jednotlivých harmonických složek signálu oproti vstupnímu signálu.
- **Šum** – je reprezentován vnitřně generovanými parazitními signály (podle druhu rušení existuje mnoho druhů – bílý šum, tepelný šum, impulsní šum).
- **Přeslechy** – interference vznikající mezi jednotlivými vodiči v kabelu.
- **Šířka pásma** – prostor mezi nejnižší a nejvyšší frekvencí, které je schopno médium přenášet (v Hz). Může být výrazně vyšší, než skutečně využívaná šířka pásma (přenosové pásmo) během přenosu.

Reálná přenosová cesta:



Primární parametry vedení:

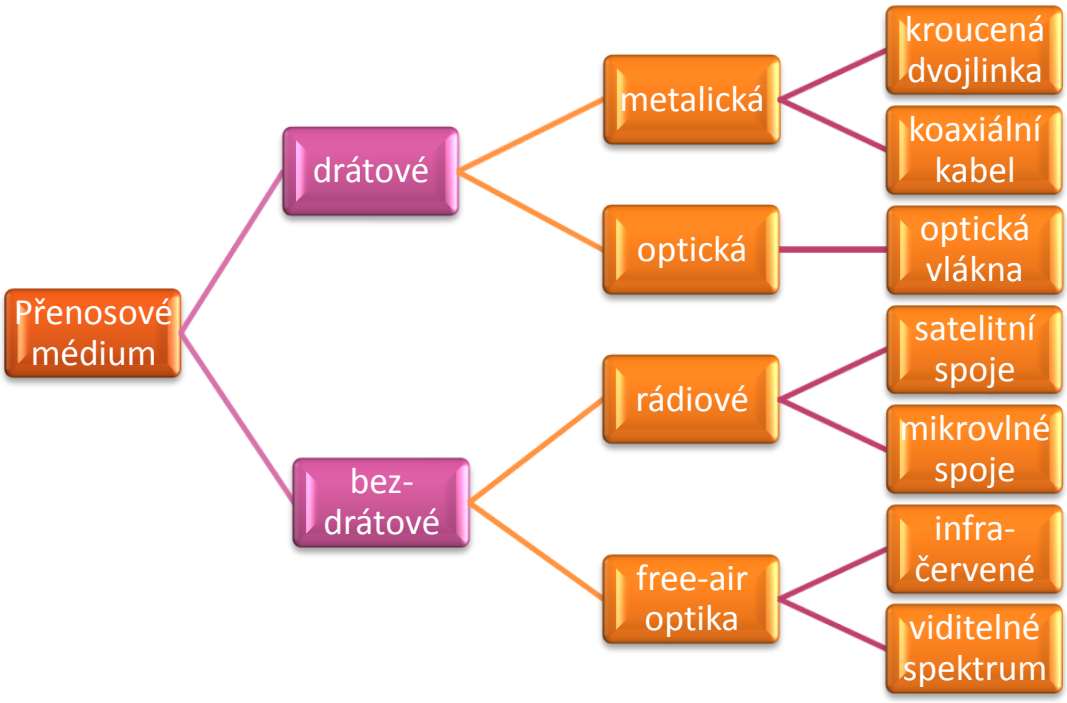
- měrný odpor R [Ω/km]
- měrná podélná indukčnost L [mH/km]
- měrná příčná kapacita C [nF/km]
- měrný svod, vodivost dielektrika G [μS/km]
- délka vedení Δx

Obrázek 1. Náhradní schéma vedení

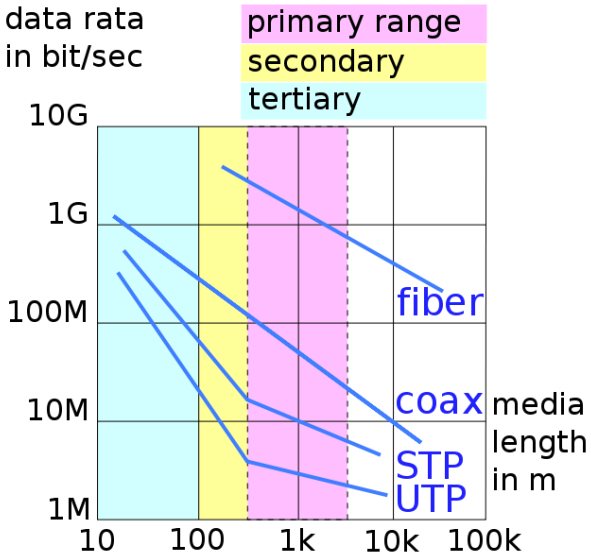
11.1 Přehled typů přenosových médií:

- Média kabelového typu:
  - kroucený dvoudrát (twist pair) – stíněný č i nestíněný
  - koaxiální kabel určený buď pro základní pásmo, nebo pro TV rozvody
  - optická vlákna jednovidová nebo mnohovidová

- Média pro přímý (nevedený) přenos:
  - elektromagnetické vlnění (vzduch, voda, vakuum)



Obrázek 2. Typy přenosových médií



Obrázek 3. Typické dosažitelné přenosové rychlosti vzhledem k délce média na jednotlivých přenosových médiích.

Otázky, úkoly

- Jaké technologie využívají kterou část spektra elektromagnetického záření pro přenos informace?
- V které části spektra lze dosahovat největších přenosových rychlostí?

- Na obrázku náhradního schéma vedení definuj, která „součástka“ způsobuje, které problémy.

Další zdroje ke studiu

Použité obrázky

[1] Autor Vojtěch Novotný

[2] Autor Vojtěch Novotný

[3] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: <http://commons.wikimedia.org/wiki/File:Speed-vs-length.svg >

12. Kroucený dvojdrát (dvojlinka)

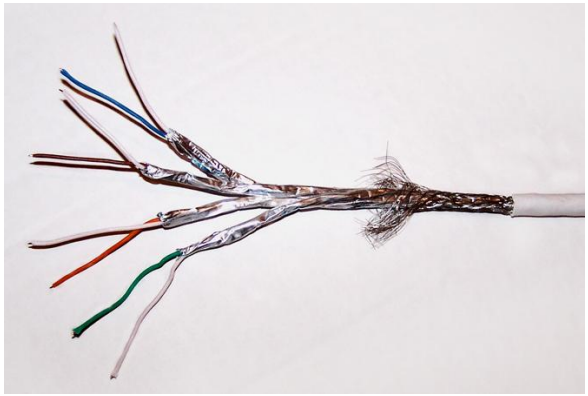
Již z názvu je zřejmé, že kroucená dvoulinka je tvořena dvěma vodiči, resp. párem vodičů. Zásadní je, že tyto vodiče jsou po celé své délce pravidelným způsobem „zkrouceny“ (anglicky: twisted, odsud také twisted pair). Oba vodiče jsou přitom rovnocenné. Výsledný užitečný signál je vyjádřen rozdílem potenciálů mezi těmito dvěma vodiči.

Symetričnosti obou vodičů zmenšuje i efekt vnějších vlivů, které na kroucenou dvoulinku mohou působit. Pokud by totiž nějaké vnější elektromagnetické pole tzv. naindukovalo ve vodičích kroucené dvoulinky elektrický potenciál, pak v obou vodičích by byl přibližně stejně velký, a vzájemně by se vyrušil (protože „užitečný" signál je dán rozdílem potenciálů obou vodičů).

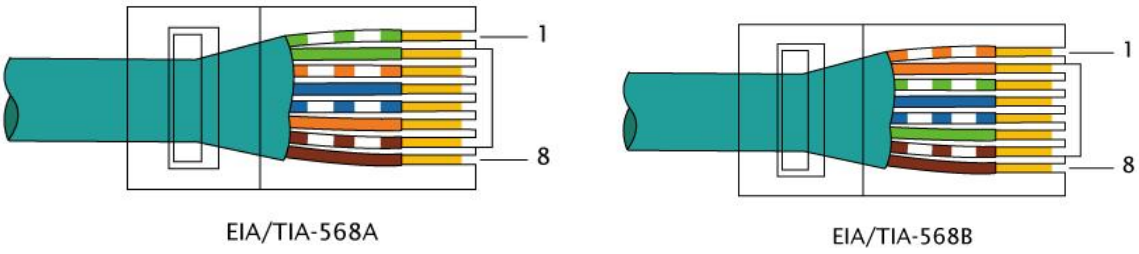
Kroucením vodičů se dále minimalizují se takzvané přeslechy mezi páry. Dva souběžně vedoucí vodiče se chovají jako anténa. Pokud je jimi přenášen střídavý signál, vyzařují do svého okolí elektromagnetické vlny. Lze je, ale výrazně snížit tím, že se oba vodiče pravidelně zkroutí. Vyzařování se tím sice neodstraní úplně, ale sníží se na takovou míru, která již může být přijatelně nízká.

Kroucená dvojlinka je dnes zdaleka nejrozšířenějším přenosovým médiem pro lokální sítě. Vyrábí ve dvojím provedení stíněný dvoudrát (STP nebo S-FTP) a nestíněný dvoudrát (UTP – unshielded twisted pair). Podle požadované kvality (odolnosti proti rušení, útlumu) se kabely vyrábějí v kategoriích označených Category 1, 2, 3,…*x*. Pro Gigabitové sítě je třeba minimálně kategorii 5e. Kabel zpravidla obsahuje 4 páry tedy 8 vodičů.

Útlum kroucené dvojlinky je od 0,5 dB/km a je závislý dle frekvence. Dle provedení dokáže přenášet signály do 700 Mhz. Maximální přenosová rychlost je 10 Gbit/s na vzdálenosti do několika metrů pak i 100 Gbit/s.



Obrázek 1. UTP kabel kategorie 7.



Obrázek 2. Zapojení konektoru 8P8C (nesprávně označovaný RJ45) norma A a B

12.1 Lanko, drát

Další dělení je podle jádra vodiče, používají dva typy – lanko a drát. Rozdíl v použití je především v tom, že lanko („licna“) je ohebnější a pevnější, takže se používá, tam kde jsou ohyby a lze očekávat mechanické namáhání, drát se používá pro běžné rozvody v lištách. S provedením drát se lépe pracuje.

Otázky, úkoly

- Definuj výhody a nevýhody kroucené dvojlinky.
- Kde je dnes kroucená dvojlinka nejpoužívanější?
- Vyzkoušej si krimpování konektoru 8P8C.
- Zjisti rozdíly mezi konektory 8P8C a RJ45.

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW:http://commons.wikimedia.org/wiki/File:UTP_CAT7.jpg

[2] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: http://commons.wikimedia.org/wiki/File:RJ-45_TIA-568A_Right.png, http://commons.wikimedia.org/wiki/File:RJ-45_TIA-568B_Right.png

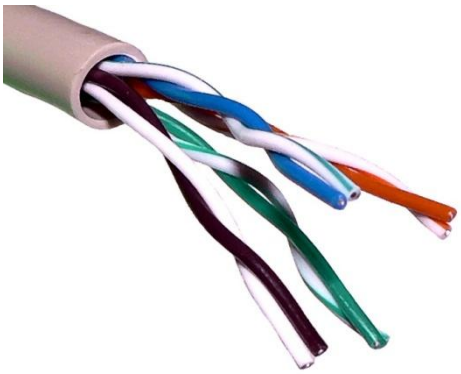
Použité zdroje

[1] Přispěvatelé Wikipedie, *Kroucená dvojlinka* [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 10. 04. 2012, 13:15 UTC, [citováno 11. 04. 2012]<http://cs.wikipedia.org/w/index.php?title=Kroucen%C3%A1_dvojlinka&oldid=8374949>

13. Krimpování konektoru 8P8C

13.1 Co je potřeba

- TP kabel potřebné délky (UTP – nestíněná kroucená dvoulinka)

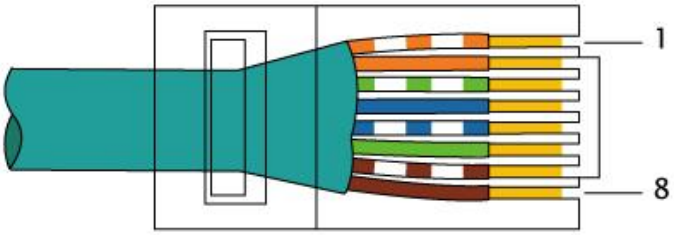


- Dva konektory RJ-45 + krytky (nejsou nutné)

- Krimpovací kleště

13.2 Postup

1. připravení kabelu, odstranění bužírky - tolik, aby se s kabely dalo pohodlně pracovat,
2. navlékneme krytku, pokud ji máme,
3. rozpleteme vodiče, aby se nám s nimi lépe pracovalo,
4. srovnáme kabely podle barviček dle normy T568B,



EIA/TIA-568B

5. zarovnáme konce a necháme jen délku potřebnou pro konektor,
6. připraveno pro nasazení konektoru,
7. při nasazování konektoru ještě zkontrolujeme, jestli se nepřehodily vodiče vodiče (barvičky),
8. konektor musí být nasazen až na doraz, bužírka musí trochu zasahovat až do konektoru, kde bude uchycena,
9. nasazený konektor vložíme do kleští a silně je stiskneme,
10. nožíky v konektoru musí být maximálně zatlačeny,
11. natáhneme krytku na konektor,
12. kontrola zapojení dle T568B,
13. a je hotovo.

Otázky, úkoly

- Vyzkoušej si krimpování konektoru 8P8C.
- Co se stane při špatném zapojení jednoho vodiče?

Další zdroje ke studiu

Video

Krimpování BNC konektoru: http://youtu.be/nKEvciE5G7c

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-05-14]. Dostupný pod licencí Creative Commons na WWW: < http://commons.wikimedia.org/wiki/File:UTP_cable.jpg>

[2] Commons.wikimedia.org [online]. [cit. 2012-05-14]. Dostupný pod licencí Creative Commons na WWW: < http://pl.wikipedia.org/wiki/Plik:Wtyk_RJ-45.jpg>

[3] Commons.wikimedia.org [online]. [cit. 2012-05-14]. Dostupný pod licencí Creative Commons na WWW: < http://pl.wikipedia.org/wiki/Plik:Zaciskarka_RJ-45.jpg>

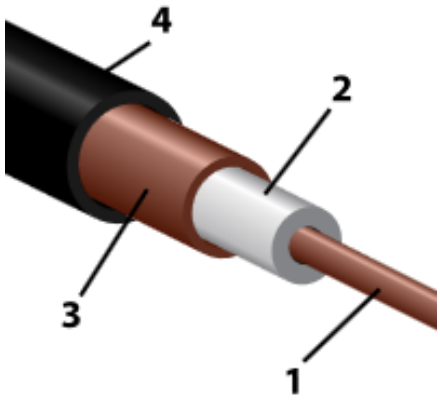
[4] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW:, http://commons.wikimedia.org/wiki/File:RJ-45_TIA-568B_Right.png

[5] Commons.wikimedia.org [online]. [cit. 2012-05-14]. Dostupný pod licencí Creative Commons na WWW: < http://pl.wikipedia.org/wiki/Plik:Pkuczynski_RJ-45_patchcord.jpg>

14. Koaxiální kabel

Koaxiální kabel je asymetrický elektrický kabel s jedním válcovým vnějším vodičem a jedním drátovým vodičem vnitřním. Vnější vodič nazýváme často stíněním a vnitřní vodič jádrem. Vnější a vnitřní vodič jsou odděleny nevodivou vrstvou (dielektrikum).

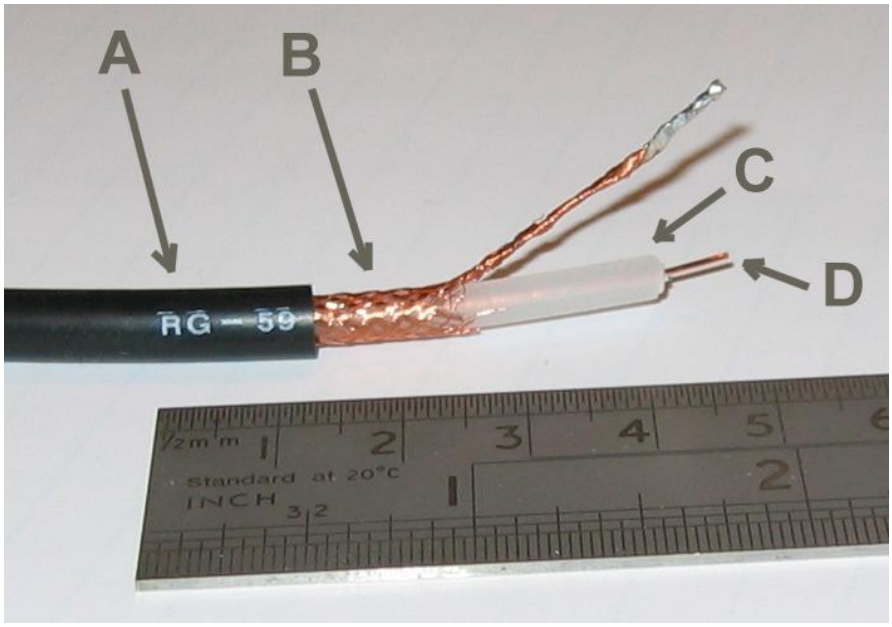
- **Vnitřní vodič** (také střední vodič, jádro) – bývá zhotoven z mědi, má podobu plného drátu nebo lanka spleteného z více drátků, u větších bývá dutý.
- **Vnější vodič** (také stínění) – bývá zhotoven z hliníkové nebo měděné fólie nebo je tvořen jako opletení dielektrika měděnými vlákny, případně kombinace obojího. Hlavní efekt vodivého opletení spočívá především v odstínění vnitřního vodiče od vlivu vnějšího rušení – koaxiální kabely jsou proto vůči rušení dosti odolné.
- **Dielektrikum** – je izolační vrstva vložená mezi vnitřní a vnější vodič. Velkou měrou ovlivňuje vysokofrekvenční vlastnosti koaxiálního kabelu. Bývá zhotoveno obvykle z polyethylenu, vzduchu, ale i jiných izolačních materiálů.



Obrázek 1. Schematická struktura koaxiálního kabelu, 1 - vnitřní vodič, 3 - vnější vodič, 2 - dielektrikum, 4 - ochranný plast

Koaxiální kabel se používal hlavně u desetimegabytového Ethernetu (mj. umožňoval vytvářet jednoduše odbočky), ale kvůli nepříznivým fyzikálním parametrům se pro rychlé lokální sítě už s koaxiálem nepočítalo. Další nevýhody oproti kroucené dvojlince jsou špatná práce s konektory i samotnými kabely.

Vodivost je elektrická. Přeslechy jsou díky stínění velmi nízké. Dle provedení přenáší signály (analogové) až do 6000 MHz! Útlum koaxiálního kabelu je asi od 3 dB/km a je značně závislý na frekvenci. Koaxiální kabel se používá pro digitální přenos obvykle na krátké vzdálenosti do rychlostí 500 Mbit/s, pro analogový přenos (kabelové televize, antény) do několika Gbit/s.



Obrázek 2. Struktura odizolovaného koaxiálního kabelu D - vnitřní vodič, B - vnější vodič, C - dielektrikum, A - ochranný plast

Obrázek 3. BNC-T konektory používané na rozbočení signálu a terminátor

Otázky, úkoly

- Definuj výhody a nevýhody koaxiálního kabelu.
- Kde je dnes kroucená koaxiální kabel nejpoužívanější?
- Co je to terminátor, proč se používá?

Další zdroje ke studiu

- http://www.earchiv.cz/a96/a643k150.php3

Video

Tester koaxiálního kabelu: http://youtu.be/IQfEUjvU4vE

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: http://commons.wikimedia.org/wiki/File:Coaxial_cable_cutaway_new.svg

[2] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: http://commons.wikimedia.org/wiki/File:RG-59.jpg

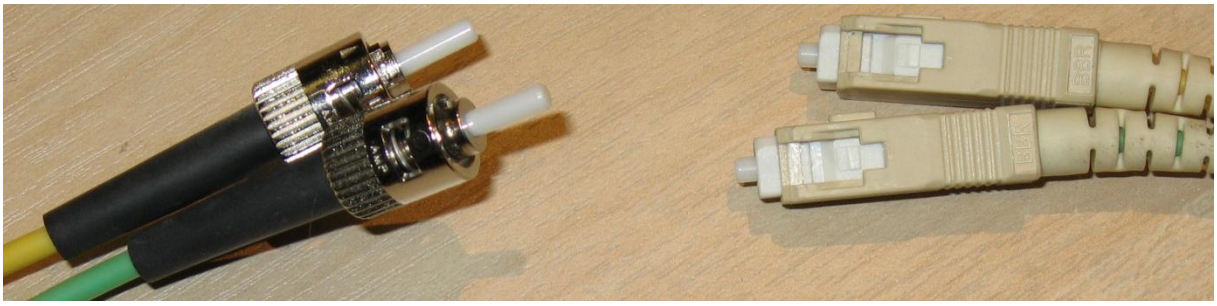
[3] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: http://commons.wikimedia.org/wiki/File:BNC-Technik.jpg

Použité zdroje

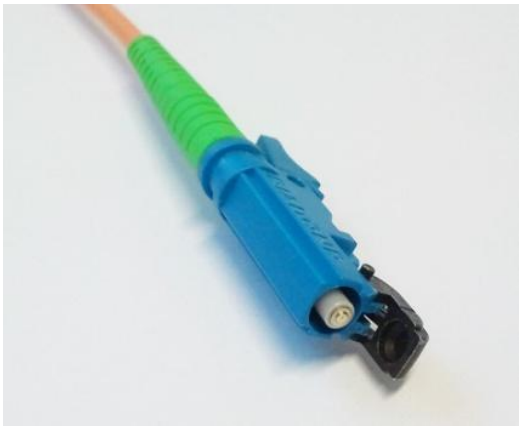
[1] Přispěvatelé Wikipedie, *Koaxiální kabel* [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 10. 02. 2012, 10:50 UTC, [citováno 11. 04. 2012] <http://cs.wikipedia.org/w/index.php?title=Koaxi%C3%A1ln%C3%AD_kabel&oldid=8077380>

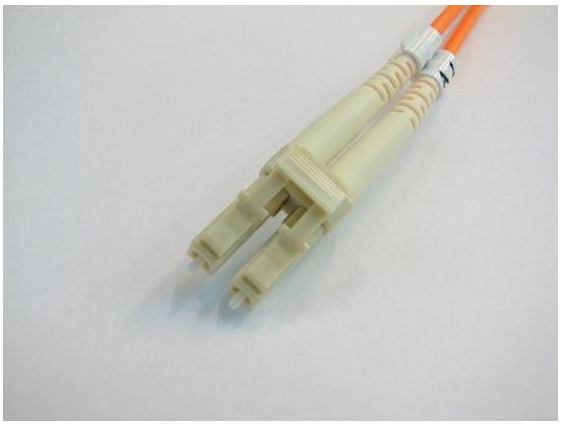
15. Optické vlákno

Optické vlákno je skleněné nebo plastové vlákno, které přenáší signály prostřednictvím světla. Vlákna se používají místo kovových vodičů, protože signály jsou přenášeny s menší ztrátou, a zároveň jsou vlákna imunní vůči elektromagnetickému rušení. Kvalitní optická vlákna jsou tedy výhodná zejména na dlouhé vzdálenosti.

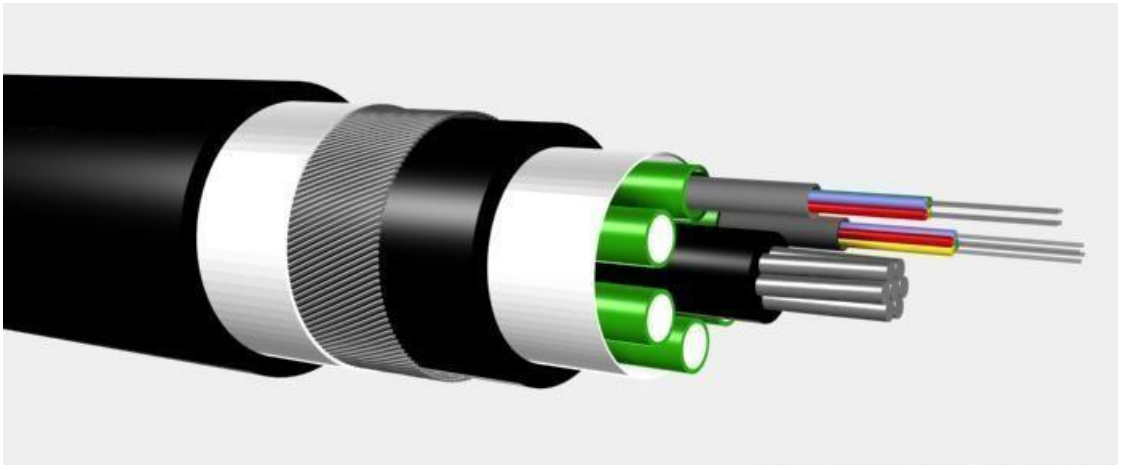


Obrázek 1. Konektory ST (nejhorší, bajonet kroutí vlákno) a SC (na ústupu.





Obrázek 2. Konektory E2000 (nejpřesnější, nejdražší, nejpoužívanější v telekomunikacích) a LC (moderní).



Obrázek 3. struktura optického kabelu s více vlánky

Díky jejich vlastnostem dosahujeme rychlosti přenosu až přes 100 Gb/s a to i na poměrně velké vzdálenosti (40 km). Každé vlákno také může přenášet mnoho nezávislých signálů, každý s použitím jiné vlnové délky světla. Telekomunikační optická vlákna mají teoretickou šířku pásma několik desítek Terabitů/s v závislosti na použitém přenosovém zařízení. Těchto rychlostí nejsme schopni dosahovat, ani zpracovávat, ale optická vlákna představují velkou rezervu do budoucnosti.

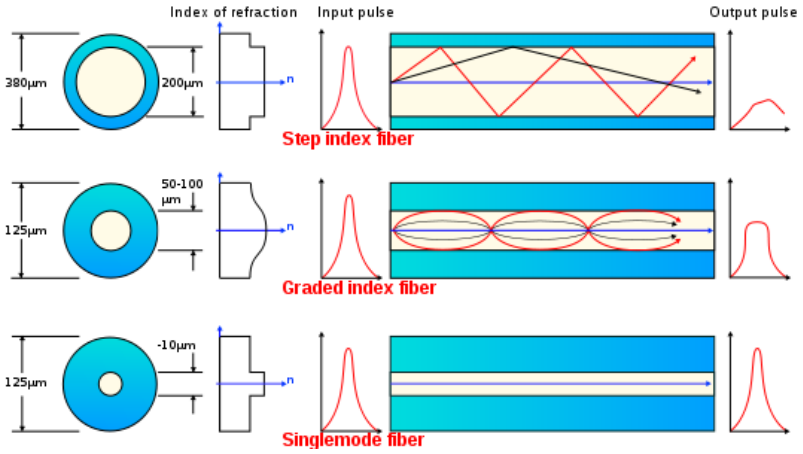
U optických vláken je složité spojování. Provádí se svařováním (drahá technika) nebo pomocí konektorů (nedokonalé spoje, vyšší útlum).

Optický kabel se skládá z následujících částí:

- **jádro:** složeno z jednoho nebo více skleněných nebo plastových vláken, kterými prochází světelný signál. Pastová vlákna jsou jednodušší na výrobu, ale je možné je použít pouze na kratší vzdálenosti.
- **plášť světlovodu:** jedná se o ochrannou vrstvu (obvykle z plastu) s nižším indexem lomu světla než má jádro.
- **obal:** vnější ochranné pouzdro.

Vyrábí se ve třech provedeních:

- **jednovidová** (SM – Single Mode), průměr je 3 až 10 mikrometrů, cena nejvyšší (nutná veliká přesnost a čistota materiálu), útlum cca 0,15 dB/km závisí na homogenitě (čistotě materiálu) je velmi malý – regenerace je každých 50 km až 100 km, zdroj světla je laser. Použití v páteřních sítích.
- **multividové vlákno s konstantním indexem lomu** (MM – MultiMode) průměr 200 mikrometrů, útlum až 50 dB/km, nejlevnější.
- **multividové vlákno s proměnným indexem lomu** (GM – GradientMode) (gradientní) průměr je 50 až 100 mikrometrů, útlum cca 0,5 až 2 dB/km, zdroj světla je LED či laser. Vlákno s proměnným indexem je vrstvené. Použití v běžných firemních sítích.

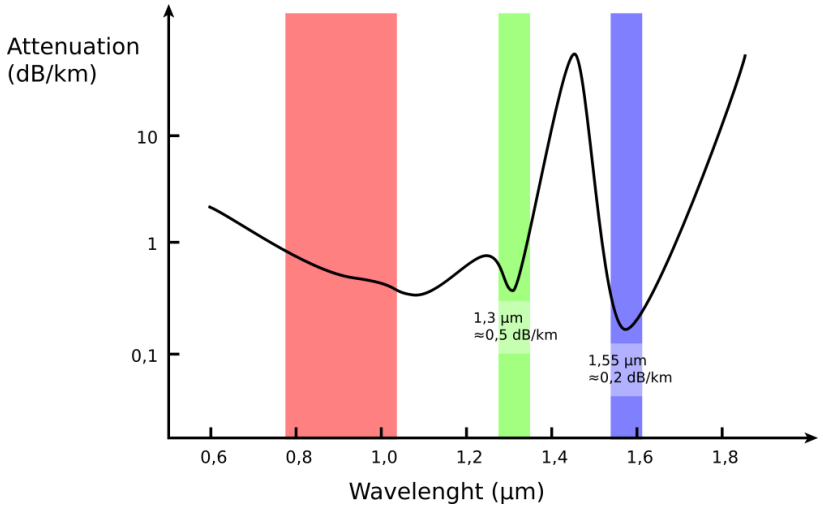


Mnohovidové vlákno se stupňovitým indexem lomu

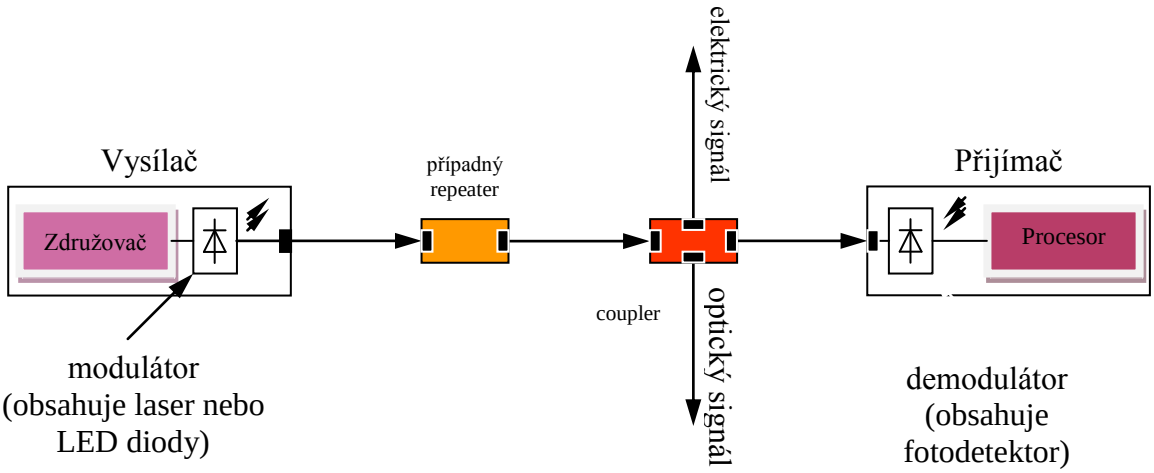
Mnohovidové vlákno s gradientním indexem lomu

Jednovidové vlákno

Obrázek 4. Způsob šíření paprsku v optickém vláknu



Obrázek 5. „Okna“ vhodná pro přenos na optickém vláknu (Útlum x vlnová délka).



Obrázek 6. Systém pro přenos informací optickým kabelem

Video

- Video montáž konektoru optického kabelu http://youtu.be/wiXi_C7ToBs
- Spojování optických vláken mechanickou cestou http://youtu.be/1YYpTCUEnC4
- Svařování optických vláken http://youtu.be/TkWMRffsKbg
- Výroba optického vlákna http://youtu.be/uSnjo5tOGQA

Otázky, úkoly

- Jaká optická vlákna používají podmořské kabely?
- Po jaké vzdálenosti je potřeba regenerovat signál na podmořském kabelu. Jak se to dělá?
- Definuj výhody a nevýhody optického vlákna kabelu.
- Najdi co nejaktuálnější mapu podmořských kabelů.
- Porovnej satelitní připojení s připojením optickým vláknem.

Použité zdroje

[2] Přispěvatelé Wikipedie, *Optické vlákno* [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 24. 02. 2012, 20:49 UTC, [citováno 11. 04. 2012] <http://cs.wikipedia.org/w/index.php?title=Optick%C3%A9_vl%C3%A1kno&oldid=8186295>

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:St-sc-fiber-connectors.jpg>

[2] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: <http://commons.wikimedia.org/wiki/File:LC-optical-fiber-connector-hdr-0a.jpg> a < http://upload.wikimedia.org/wikipedia/commons/thumb/8/88/E2000-Connector.jpg/938px-E2000-Connector.jpg>

[3] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: http://commons.wikimedia.org/wiki/File:Optical_fiber_cable.jpg

[4] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: http://commons.wikimedia.org/wiki/File:Optical_fiber_types.svg

[5] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: http://commons.wikimedia.org/wiki/File:Optical_fiber_transmission_windows.svg

[6] Autorem obrázku je Vojtěch Novotný.

16. Bezdrátové přenosy

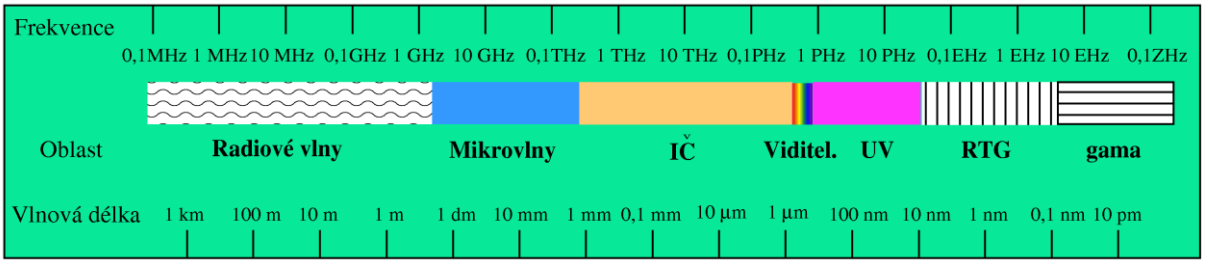
Signál se šíří volným prostorem („éterem“) prostřednictvím elektromagnetických vln. Rychlost šíření signálu dosahuje rychlosti světla to je cca 300 000 km/s.

Velkou nevýhodou je omezená-konečná dostupnost frekvencí. V jednom čase na jednom místě může probíhat jen jedna komunikace. Jinak by docházelo k vzájemnému rušení. Toto je potřeba omezovat regulací nebo technikami pro sdílením média. Za další nevýhodu můžeme považovat větší náchylnost k rušení například povětrnostními vlivy.

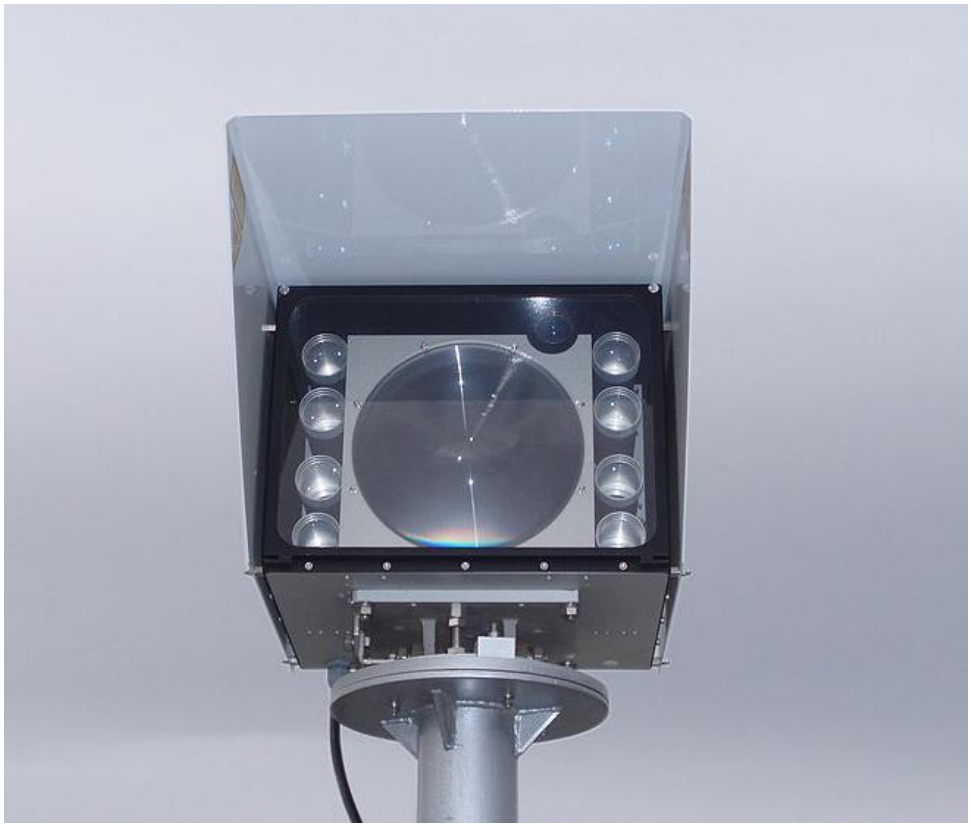
Tím, že vysíláme volně v éteru a signál se zpravidla šíří i do většího okolí lze takovouto komunikaci snadno odposlouchávat (nutno použít šifrování).

Dělení bezdrátových přenosů:

- Optické (světelné přenosy, přenosy ve viditelné části spektra)
  - Využívá se viditelná část spektra + okolí
- Infračervené
  - Frekvence nižší než červené světlo
  - Použitelné na krátkou vzdálenost s přímou viditelnosti
- Mikrovlnné
  - Vysoké frekvence (nad 100MHz)
  - Lze soustředit energii vln do svazku a ten směrovatRádiové
  - Ostatní nebo všechny



Obrázek 1. Rozdělení spektra elektromagnetického záření



Obrázek 2. Laserový vysílač/přijímač pro přenosovou rychlost 1Gb/s na vzdálenost 2 km

Obrázek 3. mikrovlnné antény

Hospodaření s frekvencemi

Frekvence jsou omezeným přírodním zdrojem, je tedy nutné s nimi hospodařit. Správcem kmitočtového spektra v ČR je ČTÚ (Český telekomunikační úřad), který spolupracuje se zahraničními subjekty a je vázán mezinárodními dohodami a úmluvami o tom, na kterých frekvencích lze provozovat které technologie.

Licenční pásmo

Je ta část frekvencí, jejíchž využití vyžaduje licencí od ČTÚ, který je přiděluje na žádost a za poplatek. Pokud je více zájemců pak v soutěži (výběrovým řízením)

Například: GSM (900MHz, 1800MHz), UMTS.

Bezlicenční pásmo

Některé části frekvencí jsou tzv. bezlicenční. Je potřeba jen dodržovat podmínky, které ČTU pro vysílání na těchto frekvencích stanovil. Určují například přípustné vysílací výkony a další parametry. Například 2,4 nebo 5 GHz pro Wi-Fi (802.11x).

Otázky, úkoly

- Proč se říká, že rádiové spektrum je národní bohatství?

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Creative Commons na WWW: <http://cs.wikipedia.org/wiki/Soubor:ElmgSpektrum.png>

[2] Commons.wikimedia.org [online]. [cit. 2012-25-08]. Dostupný pod licencí Creative Commons na WWW: <http://commons.wikimedia.org/wiki/File:FSO-gigabit-laser-link-0a.jpg>

[3] Commons.wikimedia.org [online]. [cit. 2012-25-08]. Dostupný pod licencí Creative Commons na WWW: < http://commons.wikimedia.org/wiki/File:Parabolic_antennas_on_a_telecommunications_tower_on_Willans_Hill.jpg>

Sítě LAN a MAN

Sítě LAN a MAN jsou počítačové sítě o dosahu stovek metrů až desítek kilometrů. Hlavním požadavkem je dostatečná propustnost sítě pro rychlý přenos data a případně i pro podporu služeb v reálném čase, jako hlasová služba, přenos videa, apod.

17. Ethernet

Síť Ethernet je dnes nejpoužívanější (ale ne jediný!) typ lokálních počítačových sítí. Vznikl v roce 1973 - 1980 ve výzkumném ústavu společnosti Xerox. Od doby zrodu však Ethernet prošel bouřlivým vývojem. V současnosti se však Ethernet (ve verzi gigabitového rychlejšího Ethernetu) uplatňuje i na poli metropolitních sítí.

Je standardizován skupinou standardů IEEE 802.3*x*, (*x* rozlišuje specifikace pro různé rychlosti). Existuje široká škála standardů pro různé rychlosti a určité typy vedení (viz obrázek 1).

Rychlost	Přenosové médium	Přístupová metoda
10 Mb/s	koaxiální kabel, kroucená dvojlinka	CSMA/CD, polo duplexní
100 Mb/s (Fast Ethernet)	kroucená dvojlinka, optické vlákna	CSMA/CD, polo duplexní, duplexní
1 Gb/s (Gigabit Ethernet)	kroucená dvojlinka, optické vlákna	CSMA/CD, polo duplexní, duplexní
10 Gb/s	optické vlákna, kroucená dvojlinka (do 100 metrů)	duplexní provoz
100 Gb/s	optické vlákna, kroucená dvojlinka (do 10 metrů)	duplexní provoz

Obrázek 1. Rozdělení sítí Ethernet podle rychlosti a přenosového média

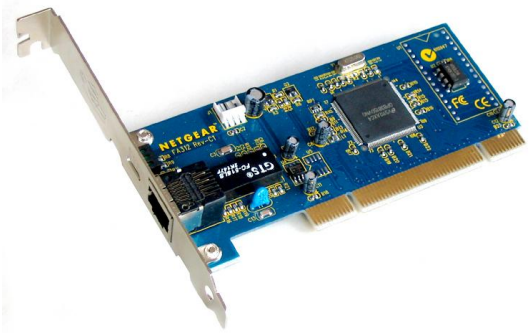
Ethernet je obecně vícebodový kabelový spoj s přístupem k médiu typu CSMA/CD nebo polo/plně duplexním provozem (od desetigigabitového ethernetu povinně). Standardy se liší především podle přenosové rychlosti a přenosového média.

Hlavními přednostmi sítě Ethernet jsou:

- široká podpora, nízká cena,
- jednoduchost technologie, snadné nasazení sítě, správa i údržba,
- možnost vytvářet rozmanité konfigurace,
- standardizovaný typ sítě zajišťující kompatibilitu produktů různých výrobců,
- zpětná kompatibilita novějších i starších variant Ethernetu.

Za nedostatek lze považovat především absenci řízení priorit v síti.

Obrázek 2. Datový rozvaděč Ethernetu.



Obrázek 3. Ethernetová síťová karta

Standardní značení standardů Ethernetu dle IEEE:

100BASE-TX

přenosová rychlost v základním pásmu typ (médium)

Otázky, úkoly

- Jaký je rozdíl mezi duplexním a poloduplexním přenosem
- Proč je Ethernenet nejrozšířenějším typem LAN sítě?

- Vyhledej jednotlivé standardy pro Ethernetu pro různé přenosové rychlosti a různá přenosová média.

Další zdroje ke studiu

- Článek o Ethernetu na serveru Svět sítí
http://www.svetsiti.cz/clanek.asp?cid=Ethernet-1992000

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

Použité obrázky

[1] Autorem je Vojtěch Novotný.

[2] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: <http://cs.wikipedia.org/wiki/Soubor:Switches_in_rack.jpg>.

[3] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: <http://cs.wikipedia.org/wiki/Soubor:NIC-FA312.jpg>.

18. Varianty Ethernetu

18.1 Desetimegabitový Ethernet

Síť Ethernet s přenosovou rychlostí 10 Mb/s je prvním standardem v řadě, který byl schválen již v roce 1983 jako standard IEEE 802.3. Existuje několik specifikací pro různé použití. Síť se vyznačuje následujícími parametry:

- přenosová rychlost 10 Mb/s,
- kódování Manchester ±0,85 V,
- přístupová metoda CSMA/CD, náhodné zpoždění mezi $2^0 – 2^{16} \times 9{,}6$ µs,
- minimální délka rámce = 512 bitů (64 B),
- fyzická adresace 48 bitů (pomoci MAC adres),
- typické přenosové médium byl koaxiální kabel, později postupně nahrazován kroucenou dvojlinkou.

18.2 Fast Ethernet (stomegabitový Ethernet)

Fast Ethernet je v principu standardní Ethernet, jen 10 krát rychlejší (100 Mbit/s). Zachovává přístupovou metodu CSMA/CD, strukturu i minimální délku rámce 64 B. Může být snadno implementován do většiny 10 Mb/s Ethernet sítí na bázi kroucené dvojlinky sítí bez nutnosti podstatných změn v kabeláži, navíc se schopností koexistence se stávající standardní sítí Ethernet 10 Mb/s.

Bylo vyvinuto několik standardů. Ve funkci kabeláže mohou být použity metalické kabely UTP kategorií 3 a vyšší a optické kabely (nikoli koaxiální kabely).

18.3 Gigabitový Ethernet

Gigabitový Ethernet byl uveden v roce 1998 a byl dalším krokem ke zvýšení přenosové rychlosti. Existují standardy jak pro kroucenou dvojlinku, tak pro optická vlákna. Zachovává přístupovou metodu CSMA/CD umožňuje poloduplexní i plně duplexní provoz. Pro představu Gigabitový Ethernet přenese jedu miliardu bitů za sekundu.

Dosah:

- kroucená dvojlinka 100 metrů,
- vícevidové optické vlákno 500 metrů
- jednovidové optické vlákno 10 – 70 km

18.4 10 Gb/s Ethernet

Desetigigabitový Ethernet (uveden v roce 2002). Je navržen pouze pro plně duplexní provoz (přístup na linku je možný kdykoliv, odpadá náhodná přístupová metoda CSMA/CD, která byl jednoznačně hlavní brzdou zrychlování. Aby totiž

systém dokázal rozpoznat kolizi, musí se signál rozšířit po celém médiu dříve, než skončí vysílání nejkratšího rámce).

Desetigigabitový Ethernet počítá se s přenosem po optických vláknech na vlnových délkách 850, 1310, 1550 nm s dosahy 65 metrů až 40 km. A do sta metrů i po kroucené dvojlince kategorie 6a a 7.

18.5 100 Gb/s Ethernet

První standardy finálně odsouhlaseny v roce 2010. Dosah 7 metrů přes měděné vodiče (kategorie 7), 125 m přes MMF a až 40 km přes SMF optické kabely. Užití pouze plně duplexního provozu. Přesto si zachovává velkou zpětnou kompatibilitu (stejný rámec, adresování,…) se standardy s nižšími rychlostmi a to uživatelé dokáží ocenit. Existují varianty dosahující jen 40 Gb/s.

18.6 1 Tb/s Ethernet

Vývoj jde neustále kupředu. Pokud nenastanou komplikace, tak je v roce 2015 očekáván 1TbE a v roce 2020 100 TbE.

Otázky, úkoly

- Přiravuje se nějaká další verze Ethernetu?

Další zdroje ke studiu

- Čtyři přednášky o Ethernetu

http://www.earchiv.cz/l218/nahled.php3?l=15&me=1

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí.* FEKT Vysokého učení technického v Brně, Brno 2006.

[2] WIKIPEDIA CONTRIBUTORS. *"Terabit Ethernet."* Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, citováno 21.9 2012. Dostupné z <http://en.wikipedia.org/w/index.php?title=Terabit_Ethernet&oldid=508463906>

19. Adresace v LAN sítích (Ethernetu)

Aby spolu mohly jednotlivé uzly v síti komunikovat, musí být jednoznačně určeno, kdo chce s kým komunikovat. K jednoznačné identifikace počítače v lokální síti se používá MAC (fyzická) adresa. MAC adresa (z anglického „Media Access Control“) je jedinečný identifikátor síťového zařízení, který používají různé protokoly druhé (spojové). Je přiřazována síťové kartě při její výrobě. Délka fyzických (MAC) adres bývá 48 bitů.

48bitové pole adresy je rozděleno na dvě stejné části (po 3 oktetech). První polovina udává kód výrobce síťového rozhraní a druhou polovinu si výrobce spravuje sám, tak aby byla zajištěna jedinečnost adresy v rámci celého světa.

MAC adresa by se měla zapisovat jako tři skupiny čtyř hexadecimálních čísel (např. 0123.4567.89ab), mnohem častěji se ale píše jako šestice dvojciferných hexadecimálních čísel oddělených pomlčkami nebo dvojtečkami (např. 01-2d-45-67-89-ab nebo 01:2d:45:67:89:ab).

Vzhledem ke skutečnosti, že moderní síťová zařízení mají možnost MAC adresu změnit, není zaručena jednoznačná identifikace zařízení v lokální počítačové síti LAN. Při výskytu zařízení se stejnou MAC adresou ve stejné lokální síti nemusí být komunikace mezi některými zařízeními plně funkční.

19.1 Zjištění MAC adresy

Windows:

Start → Spustit… → napsat cmd a do otevřeného okna napsat ipconfig /all. Vypíší se detaily všech síťových adaptérů včetně jejich MAC adres:

```
Přípona DNS podle připojení . . . : example.net
Popis . . . . . . . . . . . . . . : Realtek RTL8139/810x
Fyzická Adresa. . . . . . . . . . : 00-11-09-97-26-FE
Protokol DHCP povolen . . . . . . : Ano
Automatická konfigurace povolena  : Ano
Adresa IP . . . . . . . . . . . . : 192.168.1.153
Maska podsítě . . . . . . . . . . : 255.255.255.0
Výchozí brána . . . . . . . . . . : 192.168.1.1
Server DHCP . . . . . . . . . . . : 192.168.1.1
Servery DNS . . . . . . . . . . . : 192.168.1.1
Zapůjčeno . . . . . . . . . . . . : 9. října 2012 12:02:15
Zápůjčka vyprší . . . . . . . . . : 8. listopadu 2012 12:02:15
```

Obrázek 1. Výstup příkazu ipconfig /all ve Windows

Linux:

Přihlásit se do konzole a spustit příkaz ifconfig | grep HWadr:

```
eth0      Link encap:Ethernet  HWadr 00:15:17:e1:29:5f
```

Obrázek 2. Výstup příkazu ifconfig | grep HWadr v Linuxu

Mac OS X:

Spustit aplikaci Terminál a zadat příkaz ifconfig, popřípadě doplněný vnitřním názvem síťové karty (Ethernet zpravidla en0, AirPort en1). Vypíší se podrobnosti o síťových kartách, MAC adresa je uvozena slovem ether:

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu
1500
        ether 00:1b:63:8a:db:1a
        inet6 fe80::21b:63ff:fe8a:db1a%en0 prefixlen 64 scopeid 0x4
        inet6 2002:9320:5e05:c:21b:63ff:fe8a:db1a prefixlen 64
autoconf
        inet6 fec0::c:21b:63ff:fe8a:db1a prefixlen 64 autoconf
        inet 192.168.2.21 netmask 0xffffff00 broadcast 192.168.2.255
        media: autoselect (100baseTX <full-duplex>)
        status: active
```

Obrázek 3. Výstup příkazu ifconfig v MAC OS X.

Mobilní telefony

Zpravidla funguje zadání kódu, po kterém telefon vypíše MAC adresu WiFi rozhranní.

```
*#62209526#
```

Otázky, úkoly

- Zjisti MAC adresu svého počítače.
- Zjisti MAC adresu svého telefonu.
- Kolik MAC adres může mít počítač?

Použité zdroje

[1] Přispěvatelé Wikipedie, MAC adresa [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 16. 03. 2012, 11:44 UTC, [citováno 16. 05. 2012] <http://cs.wikipedia.org/w/index.php?title=MAC_adresa&oldid=8268439>

Použité obrázky

[1] Autorem je Vojtěch Novotný

[2] Autorem je Vojtěch Novotný

[3] Autorem je Vojtěch Novotný

20. Ostatní LAN (MAN) sítě

V průběhu vývoje sítí vznikla řada dalších typů, kam patří především sítě Token Ring, FDDI, Token Bus, Arcnet, Fibre Channel a 100VG-AnyLan. Většina z nich se však již dnes nepoužívá.

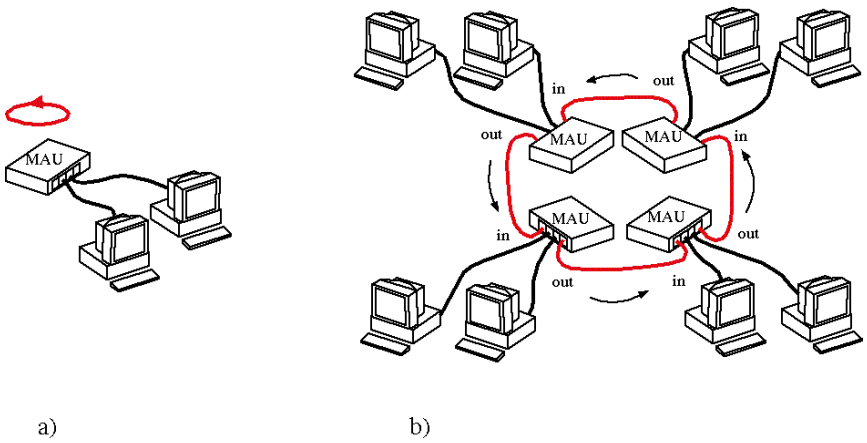
20.1 TOKEN RING

Token Ring (TR) je síť LAN s fyzickou kruhovou topologií, která byla navržena firmou IBM v 70ých letech. V současnosti existuje v několika verzích – 4 Mb/s - 1000 Mb/s. Vizuální (fyzická) topologie sítě je hvězda, která je vytvářena pomocí rozbočovacích zařízení označovaných jako MSAU (MultiStation Access Unit). Kruh je jednosměrný a může být i dvojitý, kdy druhý kruh je záložní. Stanice jsou připojeny buď pomocí UTP, STP, koaxiální či optický kabel.

Pro přístup ke sdílenému přenosovému kanálu se používá deterministická metoda předávání pověření (tokenu). Princip metody spočívá v tom, že vysílat zprávu může pouze ta stanice, která přijala pověření. Zpočátku byla tato technologie poměrně úspěšná, ale počátkem 90. let začala být vytlačována technologií Ethernetu.

V okruhu sítě je vždy jeden uzel označován jako aktivní monitor, který vykonává speciální řídicí a kontrolní funkce. Ostatní uzly jsou schopny převzít při výpadku monitoru tyto funkce automaticky. Jedná se o:

- 1. funkce generování hodinového signálu,
- 2. sledování ztráty pověření (stanice při ztrátě vynuluje okruh) a vygenerování nového token rámce,
- 3. odstraňování bloudících rámců,
- 4. vyrovnávaní frekvenčních odchylek,
- 5. pravidelná informace o přítomnosti monitoru ostatním uzlům.
- 6. inicializuje zjišťování sousedů v kruhu – důležité pro zjištění případného viníka rozpadu kruhu. Stanice, která od svého souseda neobdržela dlouho pověření, vyšle speciální zprávu (beacon) ostatním stanicím v kruhu. Stanice, která to pravděpodobně způsobila, se musí odpojit z kruhu a pak, je-li v pořádku, se opět připojit.

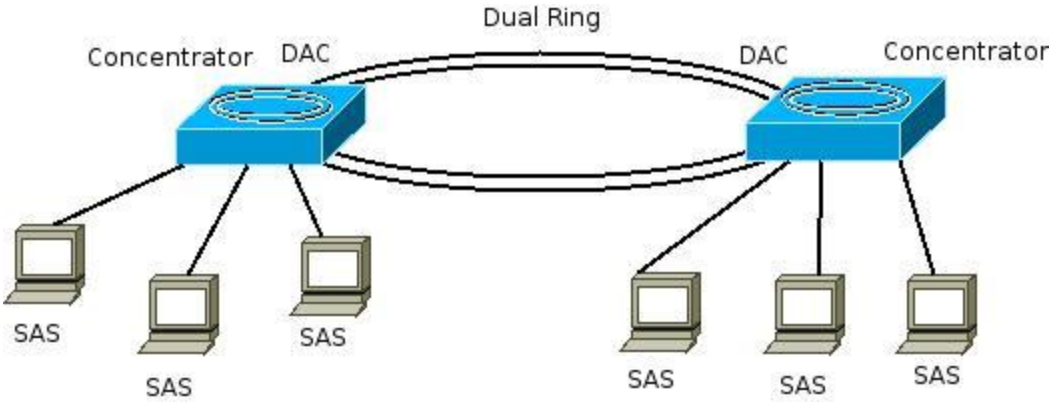


Obrázek 1. Způsob předávání dat v sítí Token Ring.

20.2 FDDI

Síť FDDI (Fiber Distributed Data Interface) je síť s kruhovou topologií. Byla to první síť s přenosovou rychlostí 100 Mb/s, která byla navržena pro sítě MAN. Byla vyvinuta v 80ých letech. Kruhová struktura je tvořena dvěma kruhy pro opačné směry přenosu, z nichž jeden je záložní pro případ přerušení kruhu. Obnova kruhu je řešena automaticky uzavřením smyčky v sousedních uzlech, mezi nimiž došlo k přerušení kruhu. Délka kruhu se tak při poruše téměř zdvojnásobí. FDDI byla navržena pro použití optických kabelů. Existuje standard i pro kroucený pár označovaný jako CDDI (Copper DDI). Přenosová rychlost je až 200 Mbit/s.

Maximální délka kruhu může být až 200 km a maximální počet stanic je 1000. Tento limit se však snižuje téměř na polovinu, chceme-li využívat výhod dvojitého kruhu. V současnosti je FDDI vytlačeno rychlými variantami Ethernetu.



Obrázek 2. Typická struktura FDDI sítě

20.3 Fibre Channel

Fibre Channel je typ sítě s relativně malým dosahem a vysokou propustností (stovky Mb/s až 20 Gb/s), která byla navržena pro propojení procesorových systémů například za účelem zvýšení bezpečnosti výpočetních systémů (clustering). Komunikace mezi dvěma uzly sítě je buď přímá (přímé propojení kabelem), nebo přepínaná anebo do kruhu. Jako přenosové médium se používají optické kabely.

Otázky, úkoly

- Proč Ethernet vytlačil Token ring a ostatní LAN sítě?

Další zdroje ke studiu

- Popis rozhranní Fibre Channel
http://www.kiv.zcu.cz/~simekm/vyuka/pd/zapocty-2004/san-mrnka/fc.html
- FDDI http://www.earchiv.cz/a97/a750k150.php3
- 100VG Any-LAN http://www.earchiv.cz/a97/a751k150.php3
- Token Ring http://www.earchiv.cz/a97/a749k150.php3
- ArcNET http://www.earchiv.cz/a97/a748k150.php3

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí.* FEKT Vysokého učení technického v Brně, Brno 2006.

[2] Přispěvatelé Wikipedie, *Fiber distributed data interface* [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 9. 02. 2012, 20:00 UTC, [citováno 11. 04. 2012] <http://cs.wikipedia.org/w/index.php?title=Fiber_distributed_data_interface&oldid=8062963>

Použité obrázky

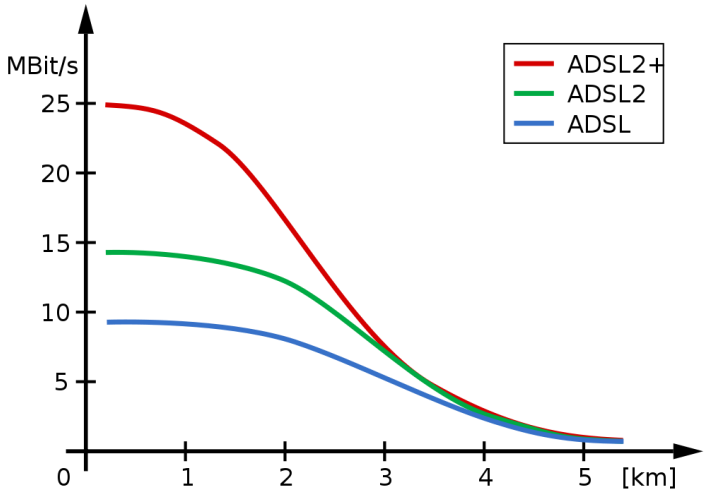
[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: <http://commons.wikimedia.org/wiki/File:Token_ring.png>.

[2] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: <http://commons.wikimedia.org/wiki/File:FDDI_Concentrator.jpeg>.

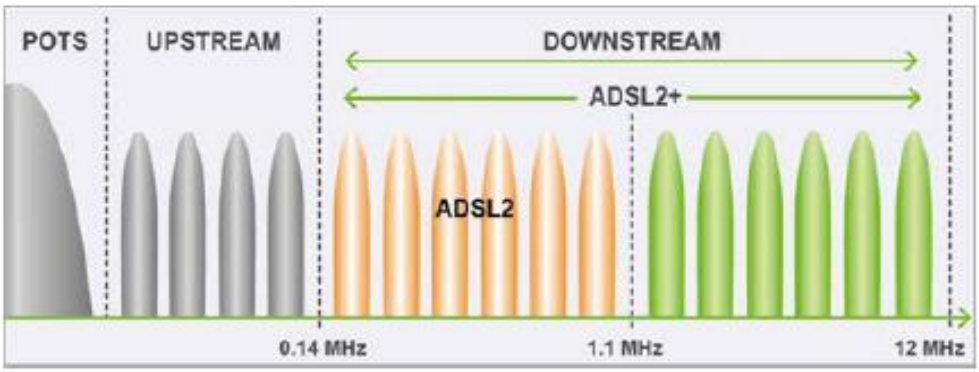
21. Další sítě (ADSL, FTTx, ATM)

21.1 ADSL, ADSL 2, ADSL 2+

- ADSL (Asymmetric Digital Subscriber Line), využívá telefonního vedení pro tzv. poslední míli telekomunikace (propojení mezi koncovým bodem sítě a účastníkem).
- dvoubodový asymetrický pronajatý spoj download max. 28 Mbit/s, upload 3,5 Mbit/s. Dosažitelná rychlost záleží na vzdálenosti účastníka od ústředny.
- zpravidla pro připojení LAN nebo PC do internetu pomocí ADSL modemu



Obrázek 1. Dosažitelné přenosové rychlosti ADSL vzhledem ke vzdálenosti



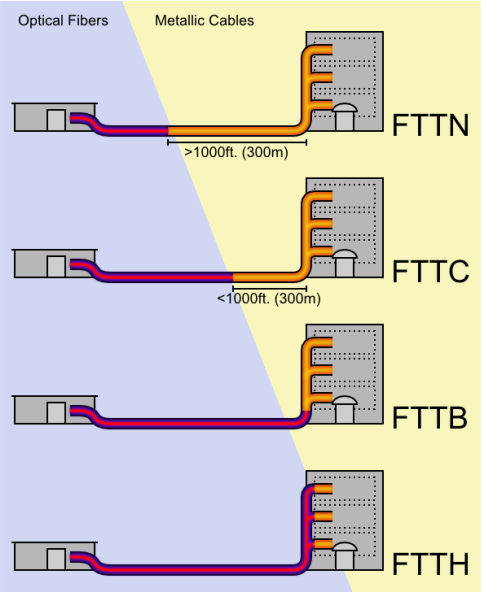
Obrázek 2. Využití spektra vedení pro ADSL

21.2 VDSL, SDSL, VDSL2

- VDSL (Very High Speed Digital Subscriber Line) nástupce ADSL,
- distribuce digitálního televizního signálu s vysokým rozlišením (HDTV),
- do vzdálenosti 300 metrů rychlost 100 Mbit/s, do 1200 metrů 12 Mbit/s (symetricky download i upload!).

21.3 FTT*x*

Fiber to the *x* (kde *x* = home, cabinet, building, node,…) je obecný pojem pro všechny druhy širokopásmové síťové architektury, která využívá optické vlákno pro nahrazení obvyklých kovových vedení, používaných pro poslední míli telekomunikace. Telekomunikační optická vlákna, která se v sítích FTT*x* používají, mají teoretickou šířku pásma několik desítek Terabitů/s v závislosti na v budoucnu použitém přenosovém zařízení. Představuje to více než 10 000 × větší přenosovou kapacitu než má metalická přípojka 1 Gbit/s. Proto optické vlákno položené v přístupové stí představuje skutečně širokopásmové médium s dostatečnou rezervou kapacity do budoucna.



Obrázek 3. Princip FTTx (x = Network, Cabinet, Building, Home)

21.4 n × 64 kb/s – E*x*, ATM, PDH, SDH, SONET

Nejpoužívanější technologie telekomunikačních operátorů vychází z násobků telekomunikačního kanálu n × 64 kb/s.

- nejčastěji odvozován ze standardu E1 = 31B+D kanál, tj. (31×64+64) kb/s,
- E1 = dvoubodový pronajatý spoj 2048 kb/s, E*x* je pak *x* krát E1,
- **ATM** je u nás využíváno jako přenosový protokol nad ADSL,
- SDH, SONET technologie uzpůsobené pro páteřní mezistátní sítě, rychlosti použité pro transport jsou pevně synchronizovány přes celou sít, pomocí atomových hodin. Tento systém dovoluje mezistátním sítím pracovat synchronně, a znatelně redukuje množství vyrovnávacích pamětí mezi jednotlivými prvky sítě,
- bývají použity k zapouzdření „slabších“ přenosových protokolů.

21.5 Kabelová televize

- využití kabelových rozvodů TV, rozšířené ve městech,
- přizpůsobení kabelové sítě pro provoz Internetu je finančně náročnější, ale většinou se vyplatí,
- technicky se provede rozdvojením klasické kabelové koncovky, kdy jedna část slouží pro příjem TV a druhá přes kabelový modem umožňuje spojení s Internetem,
- rychlost připojení v řádech desítek Mb/s a více.

21.6 Elektrická síť

- digitální komunikace po elektrické síti (PLC, angl. PowerLine Communication) a rychlý přenos dat po elektrickém vedení (BPL, angl. Broadband PowerLine),
- funguje na principu modulace datového signálu na silový rozvod 230 V,
- pro připojení je třeba PowerLine HD adaptér, který se zapojí do elektrické zásuvky,
- umožňuje šifrování pro zabezpečení připojení,
- přenosová rychlost až 200 Mb/s.
- nelze přenášet data přes transformátory.

Otázky, úkoly

- Zamysli se nad nejvhodnějším připojením pro domácnost, firmu, školu.
- Proč je ADSL asymetrické?
- Odhadni náklady na vybudování jednotlivých typů sítí.

Další zdroje ke studiu

- ATM na wikipedii
http://cs.wikipedia.org/wiki/Asynchronous_Transfer_Mode

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

[2] PŘISPĚVATELÉ WIKIPEDIE, Powerline Communication [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 19. 05. 2012, 02:56 UTC, [citováno 24. 05. 2012] <http://cs.wikipedia.org/w/index.php?title=Powerline_Communication&oldid=8551747>

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Adsl_bitrates.svg>.

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:ADSL2_frequencies.png>.

[2] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: <http://commons.wikimedia.org/wiki/File:FTTX.png>.

22. Bezdrátové sítě LAN - WLAN

Bezdrátové sítě LAN (WLAN – WIRELESS LOCAL AREA NETWORK) či MAN v posledních letech získávají stále větší oblibu, a to díky jednoduchosti a rychlosti instalace a relativně vysoké přenosové rychlosti (poslední verze (rok 2010) umožňují dosáhnout až 600 Mb/s). Bezdrátové řešení však má i své problémy, kam patří náchylnost k rušení, vícecestné šíření signálu, sdílený přístup k bezdrátovému přenosovému kanálu a další.

22.1 Bezdrátový způsob komunikace

Podstatou těchto sítí je přenos dat volným prostorem pomocí elektromagnetických vln v radiové či v optické a jí blízké oblasti spektra. Nejznámějšími standardy na poli bezdrátových sítí je řada IEEE 802.11. Lidově nazývané WiFi. Tato zkratka se často zaměňuje s výrazem IEEE802.11a/b/g/n. Jde totiž o označení a logo udělované výrobkům pracujícím podle standardu 802.11a/b/g/n, které jsou mezi sebou vzájemně propojitelné.

Pro bezdrátový způsob komunikace ve specifických citacích existují i další specifikace, jako například HomeRF, Bluetooth, sítě HIPERLAN či sítě nepočítačové založené na technologii DECT a IrDA. Pro pokrytí většího území potom například síť WiMAX.

22.2 Sítě WLAN podle standardů IEEE 802.11

Pracovní skupina IEEE 802.11 vytvořila skupinu standardů pro bezdrátové lokální sítě. Do dnešní doby byly uvolněny různé standardy definující různé přenosové rychlosti, frekvenční pásma a modulační techniky:

802.11, 802.11b, 802.11a, 802.11g, 802.11y, 802.11j, 802.11n

Přehled standardů IEEE 802.11			
Standard	Pásmo [GHz]	Max. rychlost [Mbit/s]	Fyzická vrstva
původní IEEE 802.11	2,4	2	DSSS
IEEE 802.11a	5	54	OFDM
IEEE 802.11b	2,4	11	DSSS
IEEE 802.11g	2,4	54	OFDM
IEEE 802.11n	2,4 nebo 5	600	OFDM, MIMO
IEEE 802.11ac	2,4 nebo 5	450/1300	OFDM, MU-MIMO

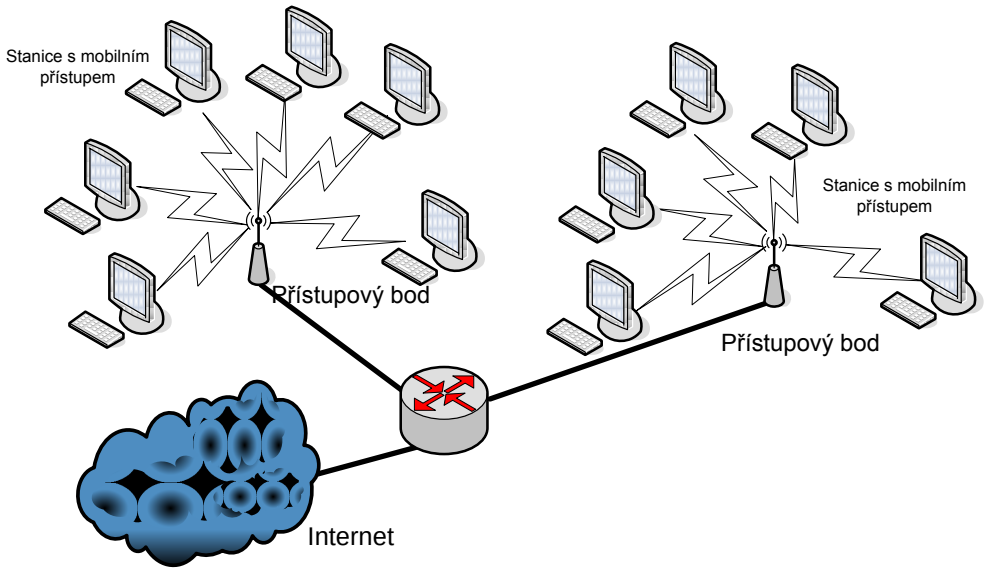
Obrázek 1. Přehled důležitých standardů IEEE 802.11

Na první pohled tyto standardy vypadají poměrně dobře a maximální rychlost se zdá být dobrá, ovšem kdyby nebyla spíše teoretická. Této hodnoty v praxi nikdy nedosáhnete.

Skutečnou rychlost ovlivňuje veliké množství faktorů od místního zarušení, vlivu počasí, překážek na cestě signálu až po samotnou fyzickou vzdálenost komunikujících klientů. Obzvláště zarušení zde sehrává obrovskou roli, protože v důsledku toho, že je ve většině případů využíváno bezlicenčního pásma, může toto spojení využívat opravdu kdokoliv, a tak lze často kdekoliv nalézt až neskutečné množství nejrůznějších bezdrátových sítí.

Další vliv na snížené reálné propustnosti má mnohem vyšší režie linkové (MAC) vrstvy ISO/OSI modelu. Oproti metalickým sítím je tato režie až několikanásobně vyšší a spotřebuje pro sebe až 30 – 40% celkové kapacity. Svou vlastní režii má též protokol TCP/IP. Reálná propustnost typicky bývá zhruba poloviční oproti přenosové rychlosti (u rychlejších standardů je to více).

Další zpoždění představuje také fakt, že už z principu komunikace v bezdrátových sítích funguje tato jako pouhý half duplex a je i tak navržena, čili buď se vysílá, nebo se přijímá, ale nikdy ne obojí najednou.



Obrázek 2. Síť s bezdrátovým přístupem k pevné síti

22.3 Acess point

Bezdrátové sítě dle IEEE802.11 využívají pro přístup stanic do sítě přístupový bod – acess point. Stanice samy mezi sebou komunikovat zpravidla nemohou. Činnost AP:

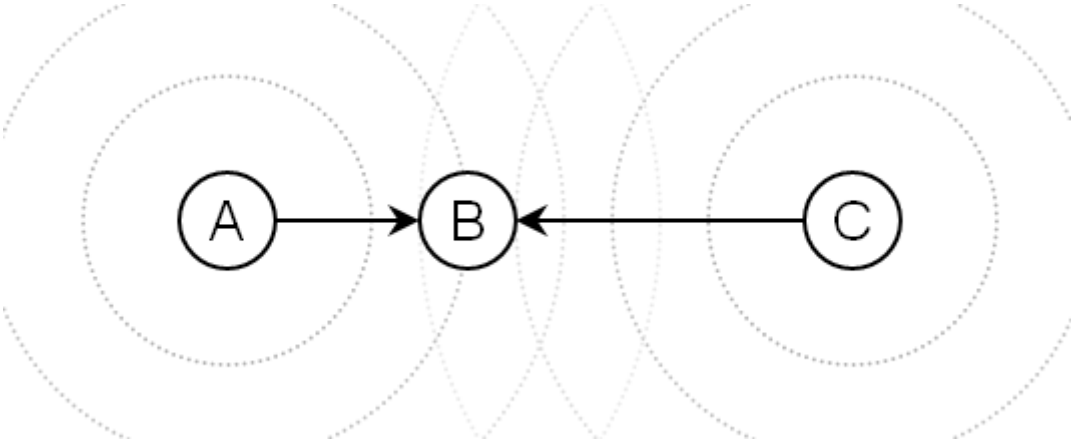
- řídí buňku
- veškeré přenosy procházejí přes AP
- ukládá rámce pro spící stanice (úspora energie)

- pravidelně vysílá Beacon Frame
- synchronizace času
- vyzývá nové stanice ke vstupu do buňky
- kdy bude vysílán další koordinační rámec (pro určení doby "sleep"),
- systémové parametry
  - pro jaké stanice má AP připravena data,
  - podporované přenosové rychlosti,
  - požadavky na schopnosti stanic,
- volitelně jméno sítě (SSID = Service Set Identifier),
- další parametry
- pravidelně 10 až 100× za sekundu.

22.4 Problém skrytého uzlu

Bezdrátové sítě musí často řešit jak předcházet problému skrytého uzlu, který představuje pro venkovní sítě poměrně velký problém.

Jde o to, že jednotliví klienti sice vidí na přístupový bod (AP), ale už vůbec nemusí vidět sebe navzájem. Není potom problém, aby začalo několik klientů vysílat ve stejné době, protože se budou domnívat, že je kmitočtové pásmo volné (na sousedního klienta přece nevidí, a tak nemohou zaregistrovat jeho vysílání). Přístupový bod se poté stává zahlceným.



Obrázek 3. Problém skrytého uzlu (A a C o sobě „neví“)

22.5 MIMO

Zvýšení rychlosti u standardu 802.11n se dosahuje mimo jiné použitím MIMO (multiple input multiple output) technologie, která využívá vícero vysílacích a přijímacích antén pro takzvaný diverzní příjem. Využívá tedy fenoménu

vícecestného šíření signálu k zvýšení propustnosti a dosahu nebo k snížení počtu přenosových bitových chyb.

Otázky, úkoly

- Jaké výhody má bezdrátový přenos a jaké nevýhody?
- Vyvíjejí se další standardy pro WiFi, jaké slibují parametry?

Další zdroje ke studiu

- Wifi http://cs.wikipedia.org/wiki/Wifi

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí.* FEKT Vysokého učení technického v Brně, Brno 2006.

Použité obrázky

[1] Autorem je Vojtěch Novotný.

[2] Autorem je Vojtěch Novotný.

[3] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Sensor_Networks_Hidden_Station_Problem.png>.

logo Wifi http://commons.wikimedia.org/wiki/File:11wifi.png

23. Zabezpečení sítí 802.11*x*

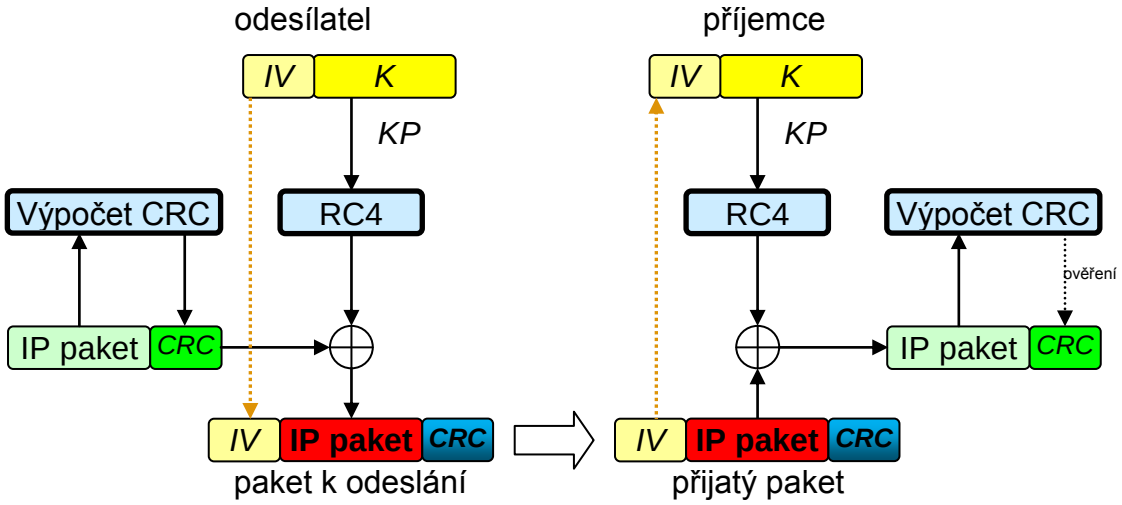
Problém bezpečnosti bezdrátových sítí vyplývá zejména z toho, že jejich signál se šíří bez ohledu na zdi budov či jiné překážky, což si mnoho uživatelů neuvědomuje. Nezvaný host se může snadno připojit i do velmi vzdálené bezdrátové sítě s pomocí dobré antény, i když druhá strana výkonnou anténu nemá. Od počátku tedy bylo jasné, že je potřeba data šifrovat. Bohužel použité šifrování má zpravidla omezenou účinnost a dá se snadno obejít.

Různé typy zabezpečení se vyvíjely postupně, a proto starší zařízení poskytují jen omezené nebo žádné možnosti zabezpečení bezdrátové sítě. Právě kvůli starším zařízením jsou bezdrátové sítě někdy zabezpečeny jen málo.

23.1 WEP

První verze zabezpečení WLAN (1999). Šifrování komunikace pomocí statických WEP klíčů (Wired Equivalent Privacy) symetrické proudové šifry RC4, které jsou ručně nastaveny na obou stranách bezdrátového spojení. Díky nedostatkům v protokolu lze zachycením specifických rámců a jejich analýzou klíč relativně snadno získat. Proto není použití WEP považováno za bezpečné.

- Paket je šifrován proudovou šifrou RC4 klíčem $KP = IV \,||\, K$ (64 bit),
- Inicializační vektor IV (24 bit) se generuje pro každý paket,
- Tajný parametr K (40 bit) je klíč přístupového bodu. Do AP i WS se vkládá ručně.
- WEP je odstrašující příklad nekompetentní implementace zabezpečení a kryptografických technik.



Obrázek 1. Šifrování WEP

Slabiny WEP

1) Klíče se vkládají lokálně a ručně a proto se málokdy mění.
2) Faktická délka klíče 40 bitů je zcela nedostatečná. Pro rychlost testování klíče 10^9 klíč/s jsou všechny klíče otestovány za $T = 2^{40}/10^9 = 18$ minut.
3) Stanice a přístupové body (AP) se neautentizují (klamné AP).
4) Použitá šifra RC4 se ukázala jako málo bezpečná (možnost luštění na PC řádově v minutách).

23.2 WPA

Kvůli zpětné kompatibilitě využívá WPA (Wi-Fi Protected Access) stejně jako WEP relativně slabý mechanizmus šifry RC4. WEP klíče, jsou ale dynamicky bezpečným způsobem měněny po určitém objemu přenesených paketů (cca 10 000). Z tohoto důvodu je možné i starší zařízení WPA vybavit.

Autentizace přístupu do WPA sítě je prováděno pomocí PSK (Pre-Shared Key – obě strany používají stejnou dostatečně dlouhou heslovou frázi) nebo RADIUS server (ověřování přihlašovacím jménem a heslem).

WPA neodstranilo některé nevýhody svého předchůdce, proto není použití ani WPA považováno za bezpečné.

23.3 WPA2

Novější (2005) WPA2 přináší kvalitnější šifrování (šifra AES), která však vyžaduje větší výpočetní výkon a proto nelze WPA2 používat na starších zařízeních. WPA2 je považováno za dostatečně kvalitní šifrování. Při požadavku na maximální zabezpečení lze použít dodatečné zabezpečení např. pomocí protokolu IPsec.

Od roku 2006 je WPA2 povinná pro všechny zařízení, které chtějí certifikaci a logo WiFi, proto není důvod toto zabezpečení nevyužívat a nezapnout ho.

23.4 Radius

V rámci tohoto protokolu se navzájem autentizuje stanice (WN) s autentizačním serverem (AS) a odvodí se klíč pro šifrované spojení WN-AP.

Postup:

1) připojení WN na nejbližší přístupový bod AP,
2) AP zprostředkuje pouze spojení WN-AS. Tato dvojice se navzájem autentizuje pomocí certifikátů. Přitom se odvodí podobně jako v TLS/SSL i klíč K pro následné šifrování WN-AP. Klíč K předá AS šifrovaně přístupovému bodu AP.
3) AP poté zprostředkuje šifrované připojení WN do LAN/Internetu.

Otázky, úkoly

- Zjisti, jak rychle jdou prolomit jednotlivé zabezpečení sítí 802.11x
- Zjisti, proč je WPA tak snadno prolomitelné.
- Kde jinde se používá šifra AES?
- Jak dodatečně zabezpečit komunikaci přes bezdrátové sítě?

Další zdroje ke studiu

- Slabá místa v zabezpečení WEP, WPA a WPA2.
http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf

Použité zdroje

[1] Přispěvatelé Wikipedie, Wi-Fi [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 4. 04. 2012, 12:43 UTC, [citováno 23. 04. 2012]<http://cs.wikipedia.org/w/index.php?title=Wi-Fi&oldid=8349596>

Použité obrázky

[1] Autorem je Vojtěch Novotný

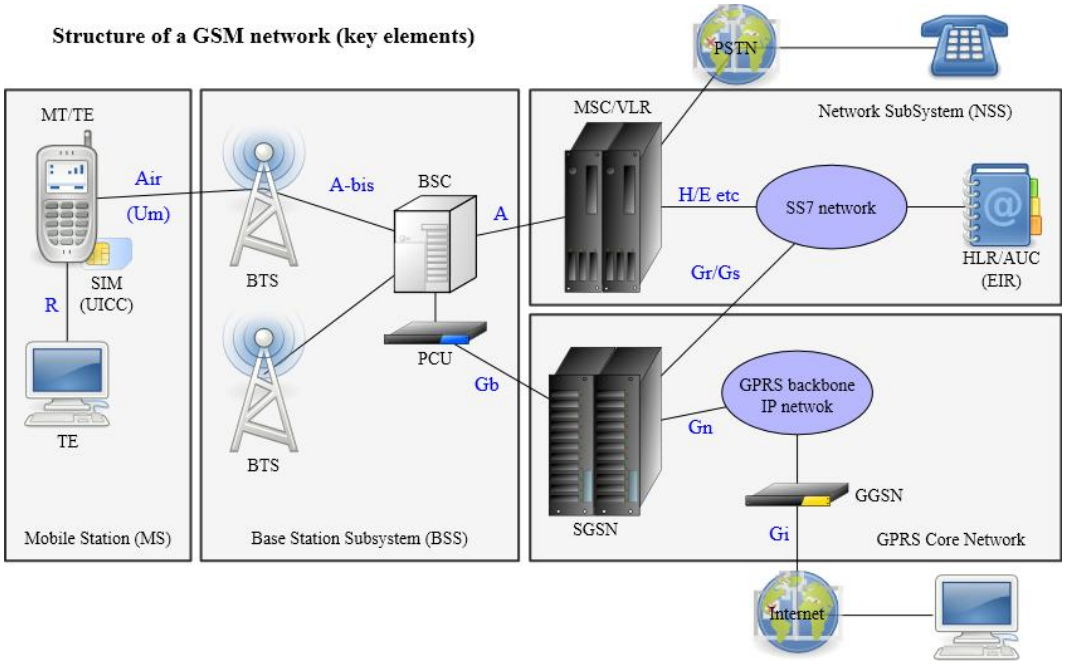
24. Další bezdrátové sítě

24.1 Bluetooth

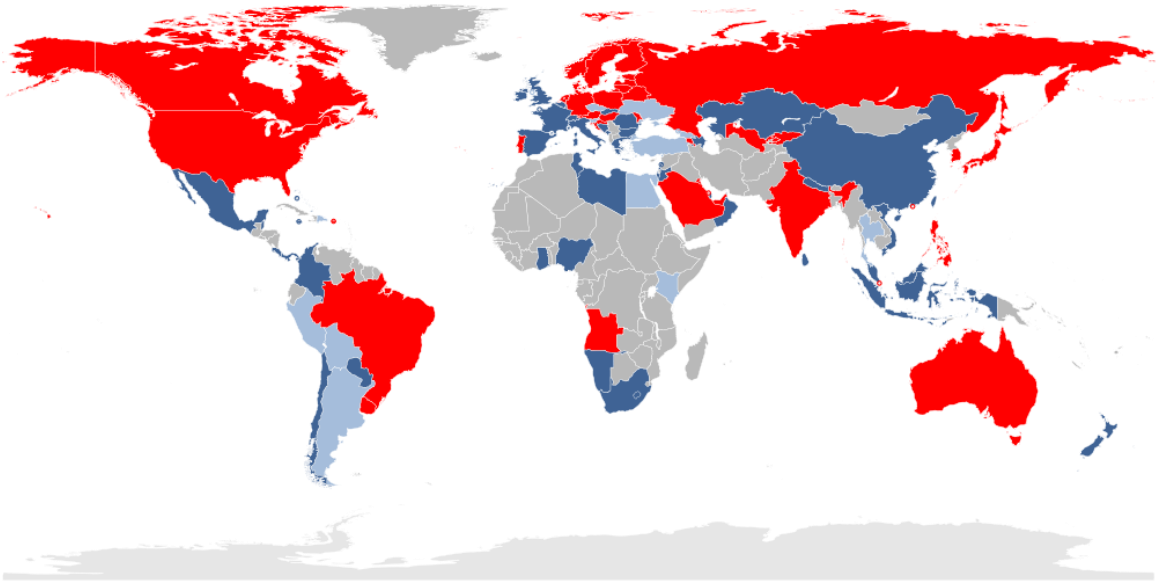
- vícebodový, většinou vlastní, rádiový spoj do 723,1 kb/s,
- jedna stanice je dočasná řídící stanice, ostatní (max. 7) jsou podřízené,
- zpravidla pro bezdrátové připojení stanic v rámci PAN, teoreticky max. 100 m.
- rádiové bezlicenční pásmo 2,40 Ghz,
- velice nízká spotřeba,
- Bluetooth 3.0 + HS (2009) teoreticky až 24 Mbit/s, ale hybridně přes WiFi.

24.2 GSM (Global System for Mobile Communications)

- dvoubodový, rádiový pronajatý spoj,
- varianty pro přímý přenos dat:
  - GPRS (General Packet Radio Service): např. (3+1) × 20 kb/s v kanálu. Maximálně 80 kbit/s.
  - EDGE (Enhanced Data Rates for GSM Evolution) – vylepšení obou předchozích systémů použitím 8stavové modulace. Někdy také nazývána EGPRS. Max 384 kbit/s, v praxi okolo 200 kbit/s.
  - UMTS (Universal Mobile Telecommunication System) – univerzální mobilní síť. Max. přen. rychlost podle rychlosti pohybu stanice až 2 Mbit/s.
  - CDMA datové přenosy na frekvenci NMT (450 Mhz). Max. až 2,4 Mbit/s.
  - HSDPA, HSPA+ technologie UMTS sítí. Maximálně až 21 Mbit/s download 5,76 Mbit/s upload.
  - LTE – (Long Term Evolution) datová mobilní síť čtvrté generace. Teoretická přenosová rychlost 326 Mb/s pro download a 86 Mb/s upload.



Obrázek 1. Struktura GSM sítě s GPRS



Obrázek 2. Stav nasazení LTE květen 2012 červená – komerční využití, tmavě modrá – probíhá stavba sítě, světle modrá – probíhá prvotní testování.

24.3 WiMAX

(Worldwide Interoperability for Microwave Access) jde o mladou bezdrátovou technologii. WiMAX je definován v řadě norem IEEE 802.16. Jde o standard pro bezdrátovou distribuci dat zaměřený na venkovní sítě.

WiMAX je otevřené řešení pro bezdrátový přístup v pásmech 2 – 11 GHz nebo 10 – 66 GHz, které díky vyspělým technologiím, vyššímu vysílacímu výkonu a použití směrových antén nabízí velký dosah signálu – teoreticky kolem 50 km při přímé viditelnosti a několik kilometrů v městské zástavbě při využití spojů bez přímé viditelnosti. Výhodou je rovněž kapacita připojení – dle verze až 268 Mb/s, kterou lze rozdělit mezi desítky klientů a každému z nich garantovat stabilní přenosovou rychlost. Další vlastností je zabudovaná podpora QoS (Quailty of Service).

Existuje také mobilní varianta WiMAXu (802.16e) dovolující komunikujícím zařízením pracovat na frekvenci 2 až 6 GHz při rychlosti pohybu až 150 km/h

Cílem WiMAXu je „poslat" WiFi sítě tam, kam původně patří, a omezit jejich použití pouze na pokrytí malých prostor, jako jsou domácnosti či firemní prostory a ač je rozšiřování této technologie pozvolné, rozhodně se jedná o krok správným směrem. Několik poskytovatelů WiMAXu lze nalézt i v České Republice.

24.4 Satelitní připojení

- Možnost „vesmírného" spojení, hlavně na zcela nedostupných místech,
- rychlost připojení v řádech Mb/s a více,
- velká latence (zpoždění) z důvodu velkých vzdáleností ke geostacionárním satelitům.

Otázky, úkoly

- Jaké výhody má bezdrátový přenos a jaké nevýhody?
- Vyvíjejí se další standardy pro WiFi, jaké slibují parametry?

Další zdroje ke studiu

- Bližší informace o WiMAX http://cs.wikipedia.org/wiki/WiMAX

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí.* FEKT Vysokého učení technického v Brně, Brno 2006.

[2] Přispěvatelé Wikipedie, WiMAX [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 17. 04. 2012, 19:16 UTC, [citováno 23. 04. 2012]<http://cs.wikipedia.org/w/index.php?title=WiMAX&oldid=8423318>

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Gsm_structures.svg>.

[2] Commons.wikimedia.org [online]. [cit. 2012-08-14]. Dostupný pod licencí Creative commons na WWW: < http://commons.wikimedia.org/wiki/File:3GPP_Long_Term_Evolution_Country_Map.svg>.

Logo Bluetooth http://commons.wikimedia.org/wiki/File:Bluetooth.svg

25. REFERENČNÍ MODEL ISO/OSI

Vzhledem ke složitosti problémů je síťová komunikace rozdělena do tzv. vrstev, které znázorňují hierarchii činností. Výměna informací mezi vrstvami je přesně definována. Každá vrstva využívá služeb vrstvy nižší a poskytuje své služby vrstvě vyšší.

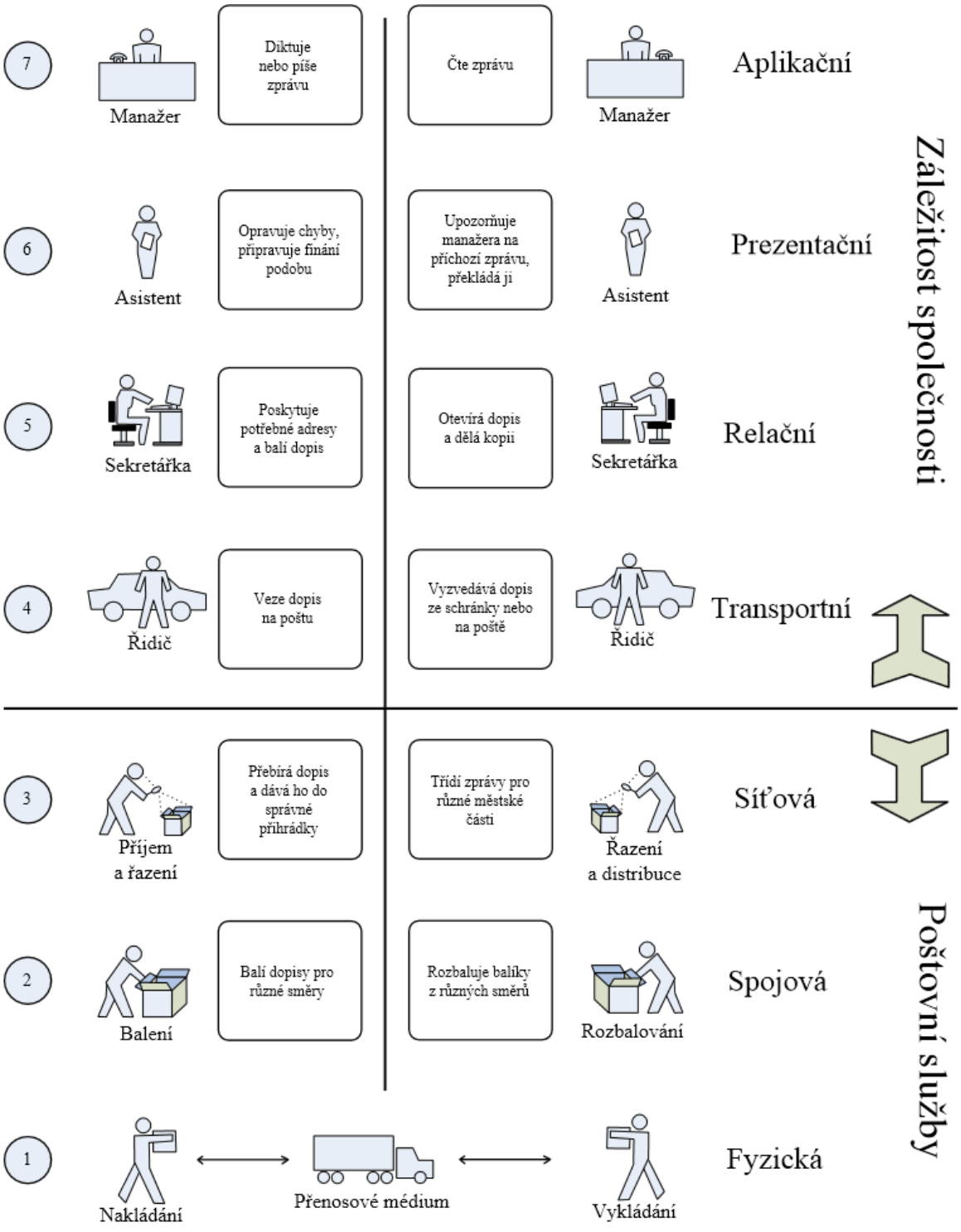
Referenční model ISO/OSI (rok 1984, OSI = Open Systems Interconnection) je nejznámější vrstvový model komplexně popisující síťovou architekturu. Představuje abstraktní model reálného otevřeného systému.

Jedná se o sedmivrstvý hierarchický model, viz obrázek níže. Model umožnil i vytváření podvrstev, což se využilo především u lokálních počítačových sítí. Pravá část obrázku zachycuje průchod zprávy jednotlivými vrstvami a označení datových jednotek na jednotlivých vrstvách.

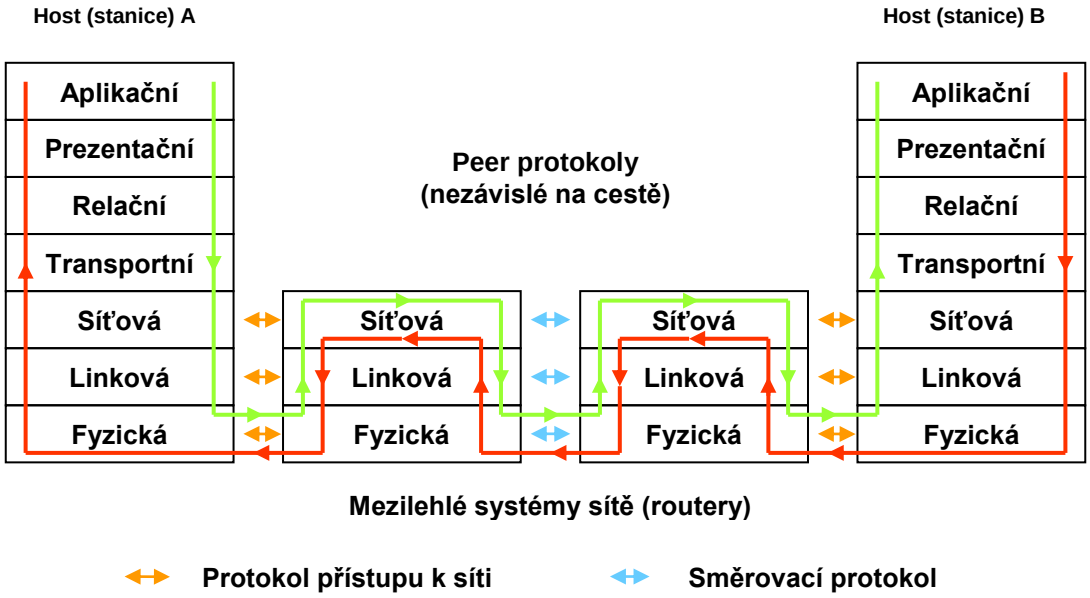
V 80. letech všeobecně považován za budoucnost sítí, oficiálně podporovaný vládou USA, přesto neuspěl.

Vrstvy modelu ISO/OSI	Typ přenášených dat	Adresace	Zařízení pracující na dané vrstvě
Aplikační	Zpráva		
Prezentační	Zpráva v přenosovém formátu		
Relační			
Transportní		Porty	
Síťová	Pakety (datagramy)	IP adresy	Směrovač
Linková	Rámce	MAC adresy	Most, Přepínač
Fyzická	Sekvence bitů		Opakovač, HUB

Obrázek 1. Model ISO/OSI



Obrázek 2. Paralela mezi distribucí dopisů a síťovým modelem ISO/OSI



Obrázek 3. Průchod dat síťovým modelem ISO/OSI

Příkladem připomínajícím vrstvový model ISO/OSI může být dopisová komunikace mezi manažery dvou firem (řekněme české a čínské). Jednotlivé vrstvy obou stran spolu zdánlivě komunikují přímo (stejné vrstvy na obou stranách používají stejný protokol, řeč, způsob prezentace dat), ale ve skutečnosti probíhá komunikace od vyšší vrstvy směrem k nejnižší, která jediná disponuje možností přenosu. Na cílové straně dochází naopak k předávání zprávy od nejnižší vrstvy směrem k vyšším.

Jednotlivé vrstvy mají kontakt (pomocí určitého rozhraní) pouze s prvky v sousedních vrstvách. Rozhraním se myslí např. poštovní schránka mezi 4. a 3. vrstvou nebo přihrádka mezi 3. a 2. vrstvou. Každý prvek na straně odesílatele zpracuje zprávu do takového tvaru (dle daného protokolu), aby jí rozuměl jeho ekvivalent na straně příjemce. Protokol např. udává, jak má být správně nadepsaná adresa 5. vrstvou, nebo jak správně ve 2. vrstvě seskupit více dopisů jdoucích stejným směrem.

Otázky, úkoly

Používá se někde ISO/OSI model tak, jak byl navržen?

Další zdroje ke studiu

- Seriál o ISO/OSI od Jiřího Peterky http://www.earchiv.cz/a92/a230c110.php3

Použité zdroje

[1] Přispěvatelé Wikipedie, Referenční model ISO/OSI [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 4. 04. 2012, 08:10 UTC, [citováno 23. 04. 2012]<http://cs.wikipedia.org/w/index.php?title=Referen%C4%8Dn%C3%AD_model_ISO/OSI&oldid=8348770>.

Použité obrázky

[1] Autorem je Vojtěch Novotný

[2] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://cs.wikipedia.org/wiki/Soubor:Rm-osi_parallel_cs.svg>.

[3] Autorem je Vojtěch Novotný

26. Fyzická vrstva

- Fyzická vrstva je nejnižší vrstvou modelu a zabývá se tedy vlastním přenosem informace prostřednictvím elektromagnetického signálu. Přenáší prostý proud bitů přenosovým médiem.
- Specifikuje fyzickou komunikaci. Aktivuje, udržuje a deaktivuje fyzické spoje mezi koncovými systémy.

Fyzická vrstva definuje všechny elektrické a fyzikální vlastnosti zařízení. Je hardwarová.

Huby, opakovače, síťové adaptéry jsou právě zařízení pracující na této vrstvě.

Fyzická vrstva definuje parametry:

26.1 Mechanické parametry

- **typ přenosového prostředí**
  - kabelové (metalické, optické kabely)
  - bezdrátové (radiové, optické)
- **vlastnosti přenosového prostředí**
  - typ kabelu, materiál kabelu, počet a průměr vodičů, pravidla pokládky kabelů, rozvody kabelové sítě,
  - maximální délka kabelu, či maximální dosah bezdrátového spoje.
- **vlastnosti rozhraní**
  - konektory – tvar, materiál, zapojení jednotlivých vodičů,
  - antény – typ.

26.2 Elektrické parametry

- **parametry signálu**
  - rychlost šíření signálu médiem, maximální zpoždění, typ signálu – analogový nebo digitální, výkonové úrovně, kódování a skramblování, modulace – analogová a digitální, polarizace, zajištění bitové a blokové synchronizace, přenosová rychlost.
- **způsob řešení duplexního provozu** – oddělený prostorově, frekvenčně, časově, kódově
- **řešení multiplexů datových toků**

26.3 Funkční parametry

- **významy signálů** jednotlivých vodičů, případně určitých bitů

26.4 Procedurální parametry

- **aktivace fyzického spoje** – nastavení parametrů přenosu – přenosová rychlost (u systémů umožňující více rychlostí přenosu), nastavení ekvalizátorů kanálu, nastolení bitové a rámcové synchronizace,
- **udržení fyzického spoje** – udržení synchronizace, přenos značek signalizujících aktivitu fyzického spoje,
- **deaktivace fyzického spoje** – pro úsporu energie v době, kdy se nic nepřenáší,
- **regenerace a rozbočení signálu** – v zesilovačích, ekvalizérech, opakovačích, rozbočovačích.

Otázky, úkoly

- Zjisti co je to skramblování.
- K čemu se používájí ekvalizátory?

Další zdroje ke studiu

- Popis fyzické vrstvy na archivu Jiřího Peterky http://www.earchiv.cz/a92/a217c110.php3

Použité zdroje

[1] Přispěvatelé Wikipedie, Referenční model ISO/OSI [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 4. 04. 2012, 08:10 UTC, [citováno 16. 05. 2012] <http://cs.wikipedia.org/w/index.php?title=Referen%C4%8Dn%C3%AD_model_ISO/OSI&oldid=8348770>

27. Linková vrstva

- Poskytuje spojení mezi dvěma sousedními systémy. Uspořádává data z fyzické vrstvy do logických celků – rámců. Opatřuje je fyzickou (MAC) adresou.
- Hlídá integritu (bezchybnost) dat pomocí kontrolních součtů.
- Linková vrstva mění prostý proud bitů na spolehlivou cestu přenosu datový ch bloků - rámců.

Seřazuje přenášené rámce, stará se o nastavení parametrů přenosu linky, oznamuje neopravitelné chyby. Formátuje fyzické rámce, opatřuje je fyzickou adresou a poskytuje synchronizaci pro fyzickou vrstvu.

Linková vrstva poskytuje funkce k přenosu dat mezi jednotlivými síťovými jednotkami a detekuje, případně opravuje chyby vzniklé na fyzické vrstvě.

Na této vrstvě pracují veškeré mosty a přepínače. Poskytuje propojení pouze mezi místně připojenými zařízeními. Je hardwarová.

V počítačových sítích bývá vrstva rozdělena do dvou podvrstev:

- podvrstva **řízení logického spoje** – LLC (Logical Link Control),
- podvrstva **řízení přístupu ke sdílenému médiu** – MAC (Medium Access Control).

Na linkové vrstvě se řeší problematika:

- **řízení komunikace** – aktivace a deaktivace linkové komunikace, potvrzování, číslování datových jednotek, řízení datového toku,
- **fyzická adresace** – nejčastěji pomocí MAC – fyzických adres,
- **zabezpečení datových jednotek** – například zabezpečení cyklickým kódem,
- **možnost multiprotokolové podpory** pro více protokolů na síťové úrovni,
- řízení přístupu ke sdílenému médiu.

Nejznámější protokol pracující na linkové vrstvě je Ethernet.

Otázky, úkoly

- Zjisti, co je to QoS.

Další zdroje ke studiu

- Popis linkové vrstvy na archivu Jiřího Peterky http://www.earchiv.cz/a92/a218c110.php3

Použité zdroje

[1] Přispěvatelé Wikipedie, Referenční model ISO/OSI [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 4. 04. 2012, 08:10 UTC, [citováno 16. 05. 2012] <http://cs.wikipedia.org/w/index.php?title=Referen%C4%8Dn%C3%AD_model_ISO/OSI&oldid=8348770>

28. Síťová vrstva

- Tato vrstva se stará o směrování paketů v síti a síťové adresování.
- Poskytuje spojení mezi systémy, které spolu přímo nesousedí.
- Síťová vrstva je jedinou vrstvou, která „vidí“ reálnou topologii rozsáhlé sítě.

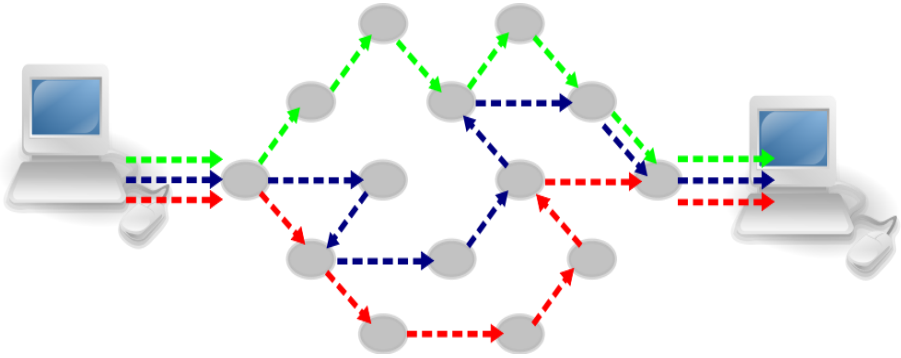
Síťová vrstva řeší problematiku směrování datových jednotek (paketů) skrze jednu případně několik vzájemně propojených různých sítí. Obsahuje funkce, které umožňují překlenout rozdílné vlastnosti technologií v přenosových sítích, a také reportuje o problémech při doručování dat.

Na síťové vrstvě pracují směrovače a posílají data do jiných sítí. Na síťové vrstvě se pracuje s hierarchickou strukturou adres. Jednotkou informace je paket. Síťová vrstva je zpravidla hardwarová, může být i softwarová.

Díky zavedení jednotného způsobu směrování sjednocuje různé sítě do jediné tzv. „intersítě“ (internet).

Vrstva realizuje:

- adresace na síťové úrovni, (dnes nejčastěji pomocí IP adres),
- překlad mezi síťovými a fyzickými adresami,
- směrování paketů na základě údajů ve směrovací tabulce,
- zajištění QoS (Quailty of Service) – upřednostnění směrování paketů služeb s vyšší prioritou,
- spojovaný/nespojovaný charakter,
- filtrování paketů (firewall) pro zavedení zabezpečení proti útokům,
- multiplex/demultiplex transportních či síťových datových toků,
- poskytování informací o stavu komunikace na síťové úrovni – dosažitelnost uzlu, doba odezvy (zpoždění ve smyčce), nedoručitelnost paketu,
- fragmentace paketů pro přenos pomalejšími kanály.



Obrázek 1. Různé pakety putují různou cestou k tomu samému cíli

Otázky, úkoly

- Zjisti, co je to QoS.

Další zdroje ke studiu

- Popis síťové vrstvy na archivu Jiřího Peterky http://www.earchiv.cz/a92/a221c110.php3

Použité zdroje

[1] Přispěvatelé Wikipedie, Referenční model ISO/OSI [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 4. 04. 2012, 08:10 UTC, [citováno 16. 05. 2012] <http://cs.wikipedia.org/w/index.php?title=Referen%C4%8Dn%C3%AD_model_ISO/OSI&oldid=8348770>

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: <http://commons.wikimedia.org/wiki/File:CPT-internet-packetswitching.svg>.

29. Transportní a relační vrstva

Transportní vrstva

- Tato vrstva zajišťuje přenos dat mezi koncovými uzly
- Transportní vrstva zvyšuje kvalitu spojů na úroveň, jakou požadují vyšší vrstvy.
- Zajišťuje komunikaci mezi jednotlivými službami (programy) koncových zařízení.

Transportní vrstva je první vrstvou nad úrovní sítě. Je zpravidla softwarová.

Řeší řadu úkolů:

- segmentace/skládání zprávy,
- určení optimální délky segmentů dat pro hladký průchod sítí,
- multiplex/demultiplex datových toků jednotlivých relací (pomocí čísel portů),
- zabezpečení bezchybnosti a úplnosti přenosu zprávy – kontrola chyb a potvrzování, skládání segmentů ve správném pořadí, odstranění zdvojených a nesprávně doručených paketů,
- konverze nespojované služby na spojovanou – budování, udržení a rozpad spojení,
- řízení datového toku – řízení intenzity vysílání zdrojového koncového uzlu,
- upřednostnění urgentních dat – přednostní zpracování důležitých dat.
- adresování pomocí virtuálních portů.
-

Vrstva nabízí obvykle spojově orientované a spolehlivé služby (TCP protokol) a nespojově orientované nespolehlivé služby (UDP protokol).

Vrstvy fyzická až transportní jsou nejčastěji součástí síťové podpory zabudované v operačním systému. Následující tři vrstvy vesměs bývají součástí určitých aplikací.

Relační vrstva

- Smyslem vrstvy je organizovat a synchronizovat komunikaci mezi spolupracujícími relačními vrstvami obou systémů a řídit výměnu dat mezi nimi.
- Umožňuje vytvoření a ukončení relací, synchronizaci a obnovení spojení, oznamovaní výjimečných stavů.

K paketům přiřazuje synchronizační značky, které využije v případě vrácení paketu (např. z důvodu, že se během přenosu dat poškodí síť) k poskládání původního pořadí. Další možností je identifikace komunikujících subjektů pro zajištění bezpečnosti přístupu k informacím.

Definuje typ komunikace (simplex, poloduplex, duplex).

Otázky, úkoly

- Co je to relace?
- Pojem port se používá na prvních třech vrstvách ISO/OSI a na vrstvě transportní. Jaký je mezi nimi rozdíl?

Další zdroje ke studiu

- Popis transportní vrstvy na archivu Jiřího Peterky http://www.earchiv.cz/a92/a224c110.php3
- Popis relační vrstvy na archivu Jiřího Peterky http://www.earchiv.cz/a92/a225c110.php3

Použité zdroje

[1] Přispěvatelé Wikipedie, Referenční model ISO/OSI [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 4. 04. 2012, 08:10 UTC, [citováno 16. 05. 2012] <http://cs.wikipedia.org/w/index.php?title=Referen%C4%8Dn%C3%AD_model_ISO/OSI&oldid=8348770>

30. Presentační a aplikační vrstva

Presentační vrstva

- Funkcí vrstvy je transformovat data do tvaru, který používají aplikace (šifrování, konvertování, komprimace).

Formát dat (datové struktury) se může lišit na obou komunikujících systémech, navíc dochází k transformaci pro účel přenosu dat nižšími vrstvami. Cílem je upravit podobu zprávy do tvaru známého oběma komunikujícím aplikačním entitám. Společné formáty textu, čísel, statických obrázků, audia a videa umožňují komunikovat aplikacím různých systémů. Mezi funkce patří např. převod kódů a abeced, modifikace grafického uspořádání, přizpůsobení pořadí bajtů apod. Řeší například háčky a čárky, CRC, kompresi a dekompresi, šifrování dat. Vrstva se zabývá jen strukturou dat, ale ne jejich významem, který je znám jen vrstvě aplikační.

Různé počítače tedy mohou používat různé způsoby vnitřní reprezentace dat. Mají-li si takové počítače svá data korektním způsobem vzájemně předávat, musí být vhodným způsobem zajištěny potřebné konverze. A ty má v referenčním modelu ISO/OSI na starosti právě prezentační vrstva.

Prezentační vrstva se tedy stará o to, aby například celé číslo bez znaménka s hodnotou 233 bylo přijato opět jako celé číslo bez znaménka s hodnotou 233, a ne např. jako celé číslo se znaménkem s hodnotou -21. Není však již úkolem prezentační vrstvy zabývat se tím, co toto číslo znamená.

Aplikační vrstva

- Účelem vrstvy je poskytnout aplikacím přístup ke komunikačnímu systému a umožnit tak jejich spolupráci
- Aplikační vrstva zpřístupňuje informačním systémům prostředí OSI.

Aplikační vrstva je nejvyšší vrstvou modelu ISO/OSI.

Aplikační protokoly podporují jednak čistě uživatelské aplikace, jako přenos souborů a poštovních zpráv nebo práci na vzdáleném zařízení, jednak administrativní aplikace (pro uživatele „neviditelné“), jako mapování jmen a adres, management sítě apod.

Aplikační vrstva implementuje protokoly tvořící jádra konkrétních aplikací, například pro přístup k webovským stránkám (HTTP), přenos souborů (FTP), elektronická služba (SMTP), aj. Aplikační vrstva řeší problematiku identifikace uživatelů, síťových zdrojů a synchronizace aplikací.

K zabezpečení služeb aplikační vrstvy jsou potřebné funkce, které jsou zahrnuty v nižších vrstvách a poskytovány formou patřící jen do aplikační vrstvy.

Na rozdíl od ostatních vrstev mohou funkce v aplikační vrstvě provádět nejen programy a technické prostředky, ale i lidé.

Otázky, úkoly

- Zjsiti jaké další protokoly, které znáš pracují na Aplikační vrstvě.

Další zdroje ke studiu

- Popis prezentační vrstvy na archivu Jiřího Peterky http://www.earchiv.cz/a92/a226c110.php3
- Popis aplikační vrstvy na archivu Jiřího Peterky http://www.earchiv.cz/a92/a227c110.php3

Použité zdroje

[1] Přispěvatelé Wikipedie, Referenční model ISO/OSI [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 4. 04. 2012, 08:10 UTC, [citováno 16. 05. 2012] <http://cs.wikipedia.org/w/index.php?title=Referen%C4%8Dn%C3%AD_model_ISO/OSI&oldid=8348770>

PROPOJOVACÍ PRVKY A MECHANIZMY

KONCENTRÁTORY

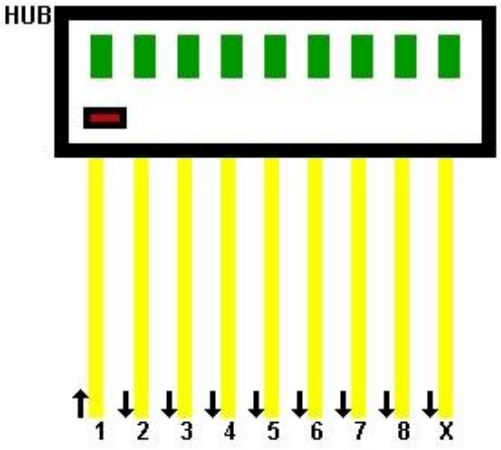
Koncentrátory vedení jsou pouze pasivní prvky umožňující vytvářet určitou schematickou topologii, například vytvoření schématu hvězda u kruhové sítě Token Ring, nebo poskytují napájení, či zajišťují překlenutí neaktivního portu v síti s kruhovou topologií.

31. OPAKOVAČE A ROZBOČOVAČE

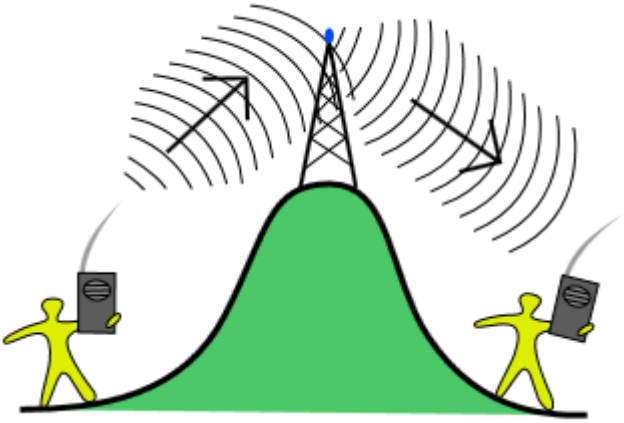
Opakovače (Repeaters) a rozbočovače (HUBs) jsou prvky pracující na fyzické úrovni vrstvového modelu sítě.

- Jejich hlavním úkolem je obnova (regenerace) signálu, tedy obnovení tvaru, časové polohy pulzů a doplnění bitové informace přidané na fyzické vrstvě (synchronizační směsi) tak, aby mohl být rámec správně přijat cílovou stanicí.
- Rozbočovač navíc dokáže rozvětvit signál do více přenosových cest.
- Rozbočovač je velmi jednoduché aktivní síťové zařízení. Nijak neřídí provoz, který skrz něj prochází.

Opakovač je zařízení se dvěma porty a rozbočovač je zařízení s mnoha porty. Signál přijatý na jednom portu je regenerován a odeslán na všechny ostatní porty (nikoliv na port původní!). Do přenosové cesty tak prvek vkládá určité, byť malé, zpoždění, jakmile detekuje 1/0 posílá signál dále – zpoždění je tedy rovno délce jednoho bitu. Je-li síť citlivá na zpoždění, je počet opakovačů (a tak i počet propojených segmentů v kaskádě) omezen. Všechny části propojené pouze opakovači (rozbočovači) tvoří jeden fyzický sdílený kanál (jednu kolizní doménu u sítí Ethernet). Všechny porty pracují se stejnou rychlostí.



Obrázek 1. Rozbočovač (HUB)



Obrázek 2. Princip opakovače

Opakovače a rozbočovače jsou pro stanice i směrovače transparentní, tj., nemají ani fyzickou a ani síťovou adresu (neobsahují-li dohledový modul) a stanice v síti tudíž o jejich přítomnosti nic neví.

Vlastnosti rozbočovačů lze shrnout do několika bodů:

- operace na fyzické vrstvě, počet portů, přenosová rychlost, typy fyzických rozhraní (koax, UTP, optika), stohovatelnost, kaskádování, modul vzdálené správy, možnost zálohy portů.

Obrázek 3. Rozbočovač (HUB)

Rozbočovače jsou již dnes na ústupu, jsou nahrazovány přepínači, které za stejnou cenu nabízejí vyšší výkony a lepší funkce.

Otázky, úkoly

- Jakou má rozbočovač nevýhodu z hlediska bezpečnosti a možného odposlouchávání?
- Co znamená, že všechny části propojené pouze opakovači (rozbočovači) tvoří jednu kolizní doménu u sítí Ethernet.

Další zdroje ke studiu

- Funkce rozbočovače http://cs.wikipedia.org/wiki/Hub

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí.* FEKT Vysokého učení technického v Brně, Brno 2006.

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Ethernet_hub.jpg>

[2] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://cs.wikipedia.org/wiki/Soubor:Repeater-schema.svg>.

[3] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://cs.wikipedia.org/wiki/Soubor:4_port_netgear_ethernet_hub.jpg>.

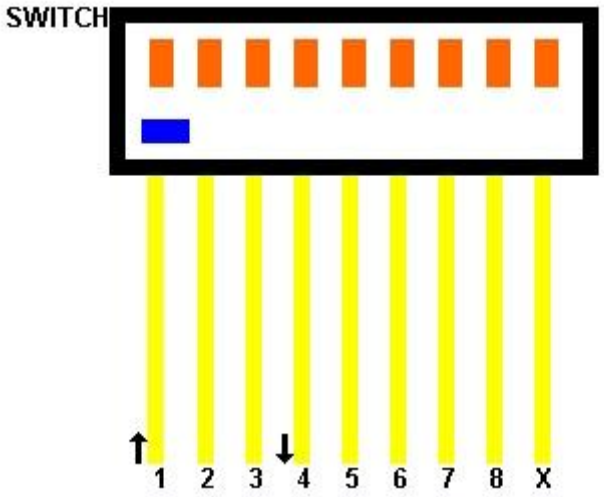
32. MOSTY A PŘEPÍNAČE

Mosty (bridges) a přepínače (switches) jsou spojovací prvky, které svoji činnost rozšiřují oproti opakovačům a rozbočovačům o linkovou vrstvu. Slouží k propojení/oddělení částí sítě mající vlastní přenosový kanál. Most je prvek se dvěma porty (byl používán dříve pro připojení segmentů k páteřní síti), přepínač je mnohaportový prvek.

32.1 Vlastnosti přepínačů

- Hlavní funkcí přepínačů je přepínání rámců na základě informací uložených v přepínací tabulce, která obsahuje vazbu mezi hardwarovou (fyzickou, MAC) adresou a svým odpovídajícím portem, kam je stanice cílová stanice připojena.

Budování přepínací tabulky je automatický proces, tedy bez zásahu člověka. Přepínač (most) si z příchozích rámců čte nejenom cílovou fyzickou adresu určující, kam se bude rámec přepínat, ale také zdrojovou adresu, a tu si spolu s číslem portu zaznamená do tabulky (pokud již tento záznam v tabulce není z dřívější doby). Přijde-li pak rámec na tuto adresu, přepínač záznam vyhledá a přepojí rámec na příslušný port.



Obrázek 4. Princip přepínače

Činnost mostů a přepínačů při příchodu rámce můžeme popsat takto:

- rámec je **zahozen**,
- je-li rámec neúplný či chybný a je-li zvolen režim s kontrolou minimální délky či s úplnou kontrolou,

- je-li určen stanici, která je připojena ke stejnému segmentu, odkud rámec přišel (není třeba nic přepínat),
- je-li přijímací vyrovnávací paměť plná,

- rámec je **přepnut** na odpovídající jiný port,
- byl-li v přepínací tabulce nalezen patřičný záznam,

- rámec je **poslán na všechny** ostatní porty,
- je-li umístění cílové stanice neznámé (není záznam v přepínací tabulce),
- je-li rámec zaslán všesměrově.

Požadavkem pro správnou funkci sítě tvořenou přepínači je stromová struktura sítě uzlů. Pokud by to nebylo dodrženo, došlo by ke zhroucení sítě. Pro zvýšení bezpečnosti se však záložní cesty budují, které je však za normální činnosti zapotřebí vypnout. O to se stará protokol označovaný jako **STP** (Spannig Tree Protocol). V případě výpadku aktivního spoje algoritmus do určité doby (řádově jednotky až desítky sekund) zajistí obnovení konektivity stromu aktivací náhradního spoje.

Výhodnou vlastností mostů a přepínačů je možnost propojení segmentů pracujících s různou přenosovou rychlostí (u sítě Ethernet např. 10/100/1000 Mb/s) a jejich automatické rozpoznání. Přepínač je za tímto účelem a pro vyrovnávání krátkodobých špiček v zatížení vybaven vyrovnávacími pamětmi.

Jde-li rozdělování a zmenšování kolizních domén tak daleko, že je na port přepínače sítě Ethernet připojena pouze jediná stanice, pak současné přepínače a síťové karty umožňují přejít od poloduplexního režimu s metodou CSMA/CD na **plně duplexní provoz**, což dále zvýší propustnost sítě.

Je nutné zdůraznit, že všechny segmenty propojené přepínači (a rozbočovači) tvoří jedinou síť, což znamená, že se celou sítí šíří všesměrové (nikoliv ostatní!) rámce s dotazy a odpověďmi (viz popis činnosti přepínače). To může při větší velikosti sítě, množství poskytovaných služeb a větším provozu dosti velkou měrou zatěžovat síť. Toto lze řešit pomocí virtuálními LAN sítěmi VLAN.

Otázky, úkoly

- Co to znamená plně duplexní provoz?
- Proč by při nedodržení stromové topologie u sítě tvořené přepínači došlo ke zhroucení sítě?

Další zdroje ke studiu

- Funkce přepínače http://cs.wikipedia.org/wiki/Switch

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Ethernet_switch.jpg>.

33. Způsob přeposílání rámce v přepínači

Z hlediska činnosti přepínačů rozlišujeme několik typů:

33.1 On the fly (Cut-through)

Přepínač načte cílovou fyzickou adresu a ihned zahájí vyhledávání cílového portu a posléze přepínání rámce. Metoda On the fly tedy začne s odesíláním ve chvíli, kdy je známa MAC adresa příjemce. Jedná se o nejrychlejší způsob přepínání, který znatelně snižuje latenci (odezvu). Skrývá v sobě však dosti podstatnou nevýhodu, a to, že přepíná i neúplné a chybné rámce, které pak zbytečně zatěžují síť.

33.2 S kontrolou minimální délky rámce

V síti Ethernet je specifikována minimální délka rámce pro správnou funkčnost přístupové metody CSMA/CD (např. 512 bitů, 64 Bytů). Přepínač tedy nejprve čeká, než přijme tuto minimální délku rámce a pak teprve, je-li rámec delší, začne s přepínáním rámce. Tak se zamezí přepínání fragmentů rámců, které byly poškozeny kolizemi.

33.3 Ulož a pošli (Store and Forward)

Celý rámec se nejprve načte do vyrovnávací paměti, pak se zkontroluje jeho bezchybnost a teprve, je-li v pořádku, dojde k jeho přepnutí. Tento režim je nejpomalejší, avšak zamezí předání jak neúplných, tak i chybných rámců. To samozřejmě snižuje zatížení sítě, protože chybná data nejsou zbytečně odeslána, nýbrž jsou zahozena.

33.4 Adaptive switching

Automatické přepínání mezi metodami cut-through switching a store and forvard dle aktuálních požadavků sítě.

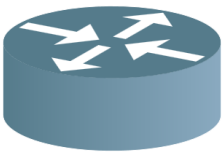
Otázky, úkoly

- Která metoda je nejvýhodnější?

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

34. Směrovače



Směrovače (routery) jsou síťové prvky zahrnující vrstvy fyzickou, linkovou a síťovou.

- Jejich hlavním úkolem je směrování paketů jednotlivými sítěmi ležícími na cestě mezi zdrojovou a cílovou sítí.
- Znalost struktury paketů také směrovače předurčuje k možnosti implementace bezpečnostních mechanizmů (firewall).
- Směrovače umožňují vytvářet složité síťové konfigurace polygonálního charakteru, které dovolují existenci více cest k danému cíli a tak zajišťují vysoký stupeň zabezpečení konektivity.

Směrovače pracují podle určitého směrovacího mechanizmu, nejčastěji se jedná o distribuovaný způsob směrování, kdy si každý směrovač buduje na základě komunikace s ostatními směrovači podle určitého **směrového protokolu** vlastní **směrovací tabulku**. Ta obsahuje záznamy určující, kam mají být pakety s určitou cílovou sítí předány. Síťová adresa se nejčastěji rozděluje na dvě, případně tři základní části (adresa sítě, adresa síťového rozhraní a případně adresa podsítě). Směrovací tabulka nese záznamy pouze o cílové síti, případně o podsíti a také běžně obsahuje záznam o implicitním směru pro směrování do sítí, pro které v tabulce neexistuje záznam. Směrovací tabulky mohou být statické či dynamické.

S vhodným softwarem (a více síťovými rozhranními) se i z obyčejného osobního počítače dá udělat router.

34.1 TTL

Může se stát, že jsou směrovací informace v tabulce některého ze směrovačů chybné. Pak může dojít k tomu, že paket nemůže být doručen a bloudí sítí. I tuto situaci směrovač efektivně řeší, a to kontrolou tzv. „doby života“ paketu. Době života odpovídá číslo v poli TTL v záhlaví paketu, které se s každým průchodem směrovačem snižuje o 1, dokud není paket doručen, nebo dokud hodnota čísla neklesne na nulu. Pak je paket zahozen, aby nezatěžoval zbytečně síť.

Obrázek 1. První Arpanetový směrovač (1969), 12KB paměti, cena 82 200$.

34.2 Statické směrovací tabulky

směrovací informace jsou uloženy do tabulky ručně při konfiguraci směrovače nebo pomocí řídicího protokolu síťové vrstvy (např. protokol ICMP sady TCP/IP). Je to vhodný způsob pouze pro jednoduché a stálé sítě. Záznam ve statické směrovací tabulce nejčastěji obsahuje tyto základní údaje:

cílová síť	maska podsítě	adresa následujícího směrovače	síťové rozhraní	stav rozhraní	četnost zpracování paketů

34.3 Dynamické směrovací tabulky

směrovací uzly si mezi sebou vyměňují pravidelně směrovací informace, čímž získávají informace o struktuře a stavu sítě, ze kterých si budují směrovací tabulky výběrem nejlepšího směru pro danou cílovou síť. To oproti statickému směrování částečně zatěžuje síť. Výměny jsou zajišťovány směrovými protokoly. V síti TCP/IP to jsou protokoly RIP a OSPF. Viz kapitolu **Chyba! Nenalezen droj odkazů.**. – Směrovací protokoly. Tento způsob je vhodný pro rozsáhlejší a často se měnící sítě. Záznam dynamické směrovací tabulky obsahuje tyto základní údaje informace:

cílová síť	maska podsítě	adresa následujícího směrovače	síťové rozhraní	cena/vzdálenost spoje	stáří směrové informace	stav rozhraní	četnost zpracování paketů

Většinou pro daný cíl existuje pouze jediný záznam, a tedy jediná cesta. Novější směrové protokoly (OSPF) však umožňují existenci více stejně vhodných cest, a tedy možnost rozložení zátěže do více cest.

34.4 Příklad funkce směrovače

Směrovací tabulka (zjednodušeně):

Síť	Maska	Next Hop	Port (Síťové rozhraní)	Metrika
192.168.1.0	255.255.255.0	192.168.254.5	Serial 1	4
10.1.2.0	255.255.255.0	Lokální rozhraní	Ethernet	0
10.5.1.0	255.255.255.0	10.10.10.2	Serial 2	3
10.5.0.0	255.255.0.0	10.5.5.5	Serial 1	2
...				
0.0.0.0	0.0.0.0	10.10.10.2	Serial 2	1

Směrovací tabulka je uspořádána sestupně podle IP adresy cílové sítě.

Směrovač po jednotlivých řádcích hledá pro přijatý paket síť, do které je adresován. Když ji najde, tak v příslušném řádku tabulky je uvedeno, do kterého portu má daný paket směrovat.

V případě více možností preferuje port s nejnižší metrikou (cenou).

Přijatý paket má cílovou adresu A = 10.5.2.1.

1. řádek: Směrovač vynásobí A×M = 10.5.2.0 ≠ S.

2. řádek: Směrovač vynásobí A×M = 10.5.2.0 ≠ S.

3. řádek: Směrovač vynásobí A×M = 10.5.2.0 ≠ S.

4. řádek: Směrovač vynásobí A×M = 10.5.0.0 = S.

Ve 4. řádku je port Serial 1 a do tohoto rozhraní je daný paket předán.

Poslední řádek znamená, že s čím si neví rady (nevyhovuje žádnému řádku) pošle směrovač na adresu výchozí brány 10.10.10.2.

Výstup příkazu *route print* ve Windows:

```
C:\Users\Vojta>route print
===========================================================================
Seznam rozhraní
 13 ...00 15 af 04 98 39 ...... Realtek RTL8187 Wireless 802.11g 54Mbps USB 2
Network Adapter
  9 ...00 17 31 8f 48 fc ...... NVIDIA nForce Networking Controller #2
  8 ...00 17 31 8f 33 8a ...... NVIDIA nForce Networking Controller
  1 ........................... Software Loopback Interface 1
 22 ...00 00 00 00 00 00 00 e0  isatap.{366514FD-0E81-4C93-BB54-A63E1B3655E4}
 23 ...00 00 00 00 00 00 00 e0  isatap.{84AFB1A5-8C16-49EF-9945-1472A76ACFD3}
 10 ...02 00 54 55 4e 01 ...... Teredo Tunneling Pseudo-Interface
 24 ...00 00 00 00 00 00 00 e0  isatap.{C9F95B23-6B09-4767-886A-6742F7AA3413}
===========================================================================

IPv4 Směrovací tabulka
===========================================================================
Aktivní směrování:
          Cíl v síti   Síťová maska            Brána        Rozhraní Metrika
          0.0.0.0          0.0.0.0    192.168.0.254     192.168.0.97    276
        127.0.0.0        255.0.0.0        Propojené        127.0.0.1    306
        127.0.0.1  255.255.255.255        Propojené        127.0.0.1    306
  127.255.255.255  255.255.255.255        Propojené        127.0.0.1    306
      169.254.0.0      255.255.0.0        Propojené      192.168.0.97     40
  169.254.255.255  255.255.255.255        Propojené      192.168.0.97    276
      192.168.0.0    255.255.255.0        Propojené      192.168.0.97    276
     192.168.0.97  255.255.255.255        Propojené      192.168.0.97    276
    192.168.0.255  255.255.255.255        Propojené      192.168.0.97    276
        224.0.0.0        240.0.0.0        Propojené        127.0.0.1    306
        224.0.0.0        240.0.0.0        Propojené      192.168.0.97    276
  255.255.255.255  255.255.255.255        Propojené        127.0.0.1    306
  255.255.255.255  255.255.255.255        Propojené      192.168.0.97    276
===========================================================================
Trvalé trasy:
  Síťová adresa            Maska    Adresa brány     Metrika
      169.254.0.0      255.255.0.0    192.168.0.240       1
      169.254.0.0      255.255.0.0     192.168.32.1       1
      169.254.0.0      255.255.0.0    192.168.160.1       1
          0.0.0.0          0.0.0.0    192.168.0.254  Výchozí
          0.0.0.0          0.0.0.0       10.1.21.10  Výchozí
===========================================================================

IPv6 Směrovací tabulka
===========================================================================
Aktivní směrování:
 Rozhraní Metrika Cíl v síti      Brána
 10     18 ::/0                     Propojené
  1    306 ::1/128                  Propojené
 10     18 2001::/32                Propojené
 10    266 2001:0:5ef5:79fd:1894:1f36:a29c:62d9/128
                                    Propojené
  8    276 fe80::/64                Propojené
 10    266 fe80::/64                Propojené
 10    266 fe80::1894:1f36:a29c:62d9/128      Propojené
```

```
  8    276 fe80::fd8c:d67c:8fc5:fbeb/128      Propojené
  1    306 ff00::/8                 Propojené
 10    266 ff00::/8                 Propojené
  8    276 ff00::/8                 Propojené
===========================================================================
Trvalé trasy:
  Žádné
```

Otázky, úkoly

- Políčko TTL se používá u IPv4, co ho nahradilo u IPv6?
- Vyzkoušej si vypsat směrovací tabulku na svém počítači, pokus se interptetovat co jednotlivé řádky znamenají.

Další zdroje ke studiu

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí.* FEKT Vysokého učení technického v Brně, Brno 2006.

Použité obrázky

[1] http://commons.wikimedia.org/wiki/File:Router.svg

[2] FICKR [online]. [cit. 2012-08-13]. Dostupný pod licencí Creative Commons na WWW: <http://www.flickr.com/photos/44124348109@N01/5114191251>.

35. Přepínání na vyšších vrstvách

Přepínání na vyšších vrstvách je též nazýváno jako „Layer/4-7 Switching“ či „Content (Web) Switching“, neboť inteligentní přepínání a rozhodování je založeno na informacích ve 4-7 vrstvě OSI modelu. Na úrovni transportní vrstvy se pracuje s přístupovými body aplikací (porty), informací na páté a šesté vrstvě modelu OSI se nevyužívá, obsah zprávy se využívá pro přepínání na úrovni vrstvy aplikační.

Nelze ale úplně správné chápat takovéto přepínání na vyšších vrstvách výhradně jako "pevné zadrátování" příslušných funkcí. Jeho hlavním cílem je skutečně výrazné celkové zrychlení, které ale může být dosaženo i jinými způsoby než jen "zadrátováním".

Příklad použití:

Směrovač funguje na síťové vrstvě, a na té má k dispozici pouze síťové adresy a základní informaci o typu nákladu (např. že na úrovni transportní vrstvy je přenášen protokolem TCP, nebo UDP). Z nich ale ještě nepozná, o jaká data se jedná a které aplikaci patří. Proto s nimi ani nemůže nakládat různé, podle toho co jsou zač.

Např. řešením je to, že se směrovači, standardně fungujícímu na úrovni síťové vrstvy, přidá schopnost analyzovat přenášený paket poněkud hlouběji - tak hluboko, aby se dostal do té jeho části, která odpovídá hlavičce transportní vrstvy, a v ní rozpoznal čísla portů odesilatele a příjemce. Z těchto čísel portů pak může usuzovat na typ přenášených dat (protože číslo portu v zásadě identifikuje aplikaci, která data generovala, resp. která má být jejich příjemcem na koncovém uzlu).

Pokud je takovýto směrovač, zkoumající přenášené pakety až do úrovně transportní vrstvy, optimalizován na rychlost podobně jako přepínač, bývá označován jako "přepínač na 4. vrstvě" (Layer 4 Switch).

Jaké ale jsou konkrétní možnosti využití "přepínače na 4. vrstvě"? K čemu přesně využít to, že rozpozná, o jaká data se jedná?

Představme si jako příklad síť, ve které je provozován WWW server. Pokud intenzita požadavků na tento server dlouhodobě výrazně vzroste, je možné ji kompenzovat zvýšením výkonnosti samotného serveru. To ale často není možné dělat libovolně dlouho. V určitém okamžiku se stává výhodnějším použít jiné řešení - například zdvojit WWW server (nahradit jeden původní server dvěma či několika identickými zařízeními), a snažit se rozkládat mezi ně zátěž co nejrovnoměrněji, tak aby byly všechny servery vytíženy pokud možno stejně.

K vhodnému rozkladu zátěže je ale nutné správě rozpoznat, že se jedná o požadavek na WWW server na určité konkrétní adrese - což se pozná jednak ze síťové adresy uzlu a dále z toho, že příslušný požadavek je na úrovni transportní vrstvy adresován portu č. 80 (na kterém standardně čeká na svá data WWW server). K tomu je nutné již přepínání na 4. vrstvě.

BRÁNY

Brány (Gateway) jsou propojovací prvky zajišťující komunikaci mezi sítěmi s odlišnými síťovými a vyššími protokoly. Brány tedy zajišťují konverzi mezi protokoly na všech vrstvách síťového modelu. Příkladem může být propojení poštovních systémů sady TCP/IP a ISO/OSI tzv. e-mailová brána, nebo propojení sítě ISDN a TCP/IP sítě pro realizaci telefonního spojení.

Otázky, úkoly

- Obejdou se dnes velké webové servery bez přepínání na vyšších vrstvách?

Další zdroje ke studiu

- Jiří Peterka - Layer 2/3/4-7 switching
http://www.earchiv.cz/b02/b0200001.php3

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

[2] PETERKA, Jiří. *Layer 2/3/4-7 switching* [online]. 2002 - 2011, [citováno 24. 8. 2012]. <http://www.earchiv.cz/b02/b0200001.php3>.

36. Architektura TCP/IP

V současnosti je s drtivou převahou nejpoužívanější protokolová sada vyšších vrstev sada TCP/IP (Transmission Control Protocol/Internet Protocol), díky tomu, že je hlavním komunikačním protokolem používaným v síti Internet.

Hlavní odlišnosti mezi referenčním modelem ISO/OSI a TCP/IP vyplývají především z rozdílných výchozích předpokladů a postojů jejich tvůrců. Při koncipování referenčního modelu ISO/OSI měli hlavní slovo zástupci spojových organizací. Ti pak nově vznikajícímu modelu vtiskli svou vlastní představu - především spojovaný a spolehlivý charakter služeb, poskytovaných v komunikační podsíti (tj. až do úrovně síťové vrstvy, včetně).

Jinými slovy:

ISO/OSI model počítá se soustředěním co možná nejvíce funkcí, včetně zajištění spolehlivosti přenosů, již do komunikační podsítě, která v důsledku toho bude muset být síť poměrně složitá, zatímco k ní připojované hostitelské počítače budou mít relativně jednoduchou úlohu. Později se ale ukázalo, že například právě v otázce zajištění spolehlivosti to není nejšťastnější řešení - že totiž vyšší vrstvy nemohou považovat spolehlivou komunikační podsíť za dostatečně spolehlivou pro své potřeby, a tak se snaží zajistit si požadovanou míru spolehlivosti vlastními silami. V důsledku toho se pak zajišťováním spolehlivosti do určité míry zabývá vlastně každá vrstva referenčního modelu ISO/OSI.

Tvůrci protokolů TCP/IP naopak vycházeli z předpokladu, že zajištění spolehlivosti je problémem koncových účastníků komunikace, a mělo by tedy být řešeno až na úrovni transportní vrstvy. Komunikační podsíť pak podle této představy nemusí ztrácet část své přenosové kapacity na zajišťování spolehlivosti (na potvrzování, opětné vysílání poškozených paketů atd.), a může ji naopak plně využít pro vlastní datový přenos.

Vývoj TCP/IP probíhal od počátku 70. let. Byla založena na těchto zásadách:

- vývoj TCP/IP směřuje od jednoduššího ke složitějšímu,
- **síť nemusí být spolehlivá, musí však být co nejrychlejší**. To znamená, že může docházet ke ztrátě paketů a spolehlivost si zajišťují až koncové uzly sítě, a to až na transportní či vyšší vrstvě, pokud je spolehlivost vyžadována. Pro zajištění spolehlivosti musí mít koncový uzel vyrovnávací paměti pro případ žádosti o opakování,
- upřednostňuje se nespojovaný charakter komunikace na úrovni sítě, tedy síť poskytuje nespojované a nespolehlivé služby. Spojovaný charakter komunikace si vytváří opět až koncový uzel sítě, je-li to nezbytné.

- vrstvový model TCP/IP neobsahuje vrstvy relační a presentační jako model OSI, protože tyto služby těchto vrstev nejsou využívány všemi aplikacemi, a v takových případech zbytečně zvyšují režii přenosu a tedy užitečný přenosový výkon sítě. Aplikace, které tyto služby vyžadují, si je samy musí implementovat.

Otázky, úkoly

Za jakých okolností nemusí počítač komunikovat přes protokol TCP/IP?

Další zdroje ke studiu

- Historie TCP/IP http://www.earchiv.cz/l223/slide.php3?l=1&me=8

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

37. Vrstvová struktura modelu TCP/IP

Problematika komunikace je z pohledu této sady rozdělena do 4 vrstev (na rozdíl od systému OSI, který je 7vrstvý), viz obrázek 1:

<table>
<tr><th>TCP/IP</th><th>Model ISO/OSI</th></tr>
<tr><td rowspan="3">Aplikační vrstva</td><td>Aplikační vrstva</td></tr>
<tr><td>Prezentační vrstva</td></tr>
<tr><td>Relační vrstva</td></tr>
<tr><td>Transportní vrstva</td><td>Transportní vrstva</td></tr>
<tr><td>Síťová (IP) vrstva</td><td>Síťová vrstva</td></tr>
<tr><td rowspan="2">Vrstva síťového rozhraní</td><td>Linková vrstva</td></tr>
<tr><td>Fyzická vrstva</td></tr>
</table>

Obrázek 1. Srovnání referenčních model TCP/IP a ISO/OSI

37.1 Vrstva síťového rozhraní

Při návrhu TCP/IP se autoři rozhodli nevymýšlet již jednou vymyšlené. Rozhodli se, že pro vrstvu síťového rozhraní se budou dát využít již existující protokoly pro LAN sítě. Vrstva síťového rozhranní tedy není blíže specifikována touto sadou, neboť je závislá na použité přenosové technologii (Ethernet, Token ring, ATM, dvoubodový spoj…). Zajišťuje vysílání a příjem paketů do/ze sítě.

37.2 Síťová vrstva (často také IP vrstva nebo mezisíťová vrstva)

zajišťuje směrování paketů po síti, sjednocuje různé typy sítí na úrovni směrování a to tak že: struktura datové jednotky = IP paket a adresování = IP adresa. Poskytuje nespojovanou a nespolehlivou službu. Funkce vrstvy jsou realizovány např. protokoly IP, ICMP, ARP a RARP, OSPF a IGMP a dalšími.

37.3 Transportní vrstva (TCP vrstva)

realizuje a zajišťuje komunikaci koncových uzlů. Mulitplexuje (ve směru do sítě) a demultiplexuje (ve směru ze sítě) datový tok od/k jednotlivých/-ým

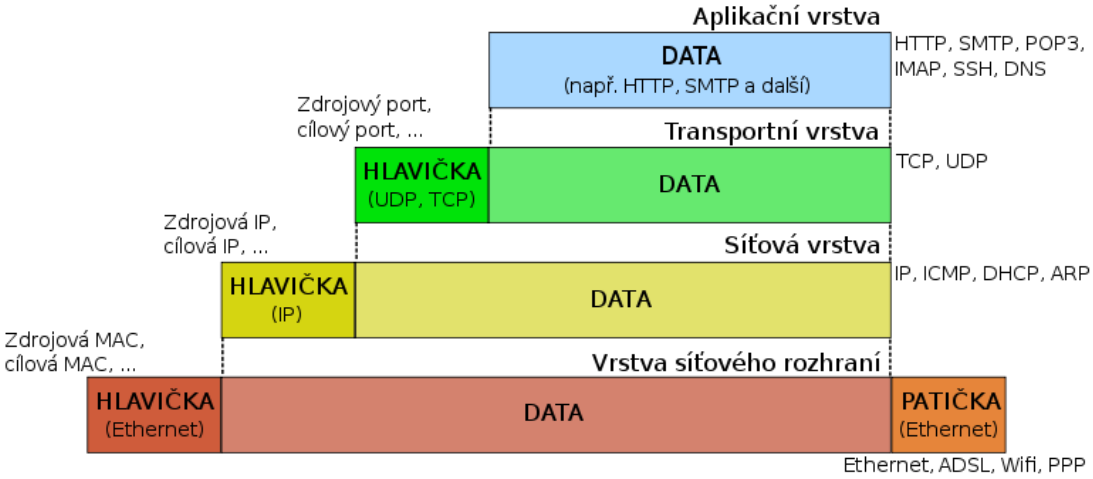
aplikací/-ím. S entitami aplikační vrstvy komunikuje přes přístupové body, tzv. porty.

Nabízí 2 služby z hlediska spojení:

- **spojově orientovanou, spolehlivou** – protokol TCP
- **nespojově orientovanou, nespolehlivou** – protokol UDP

37.4 Aplikační vrstva

– obsahuje protokoly nejčastěji používaných služeb, např. SMTP , FTP, TELNET, DNS, DHCP,…



Obrázek 2. Zapouzdření dat v síti TCP/IP

Otázky, úkoly

Porovnej výhody a nevýhody modelů ISO/OSI a TCP/IP

Další zdroje ke studiu

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-05-14]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Porovn%C3%A1n%C3%AD_TCPIP_a_modelu_ISOOSI.jpg>.

[2] Commons.wikimedia.org [online]. [cit. 2012-05-14]. Dostupný pod licencí Public domain na WWW: < http://cs.wikipedia.org/wiki/Soubor:Tcpip_zapouzdreni.svg>.

38. ADRESOVÁNÍ V PROSTŘEDÍ IP SÍTÍ

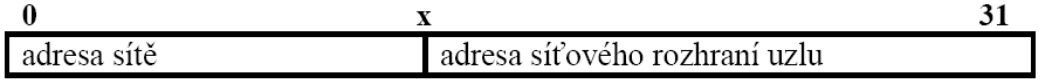
Sada protokolů TCP/IP používá pro adresování konkrétního procesu v síti 2 čísla, která jsou však umístěna v protokolech různých vrstev:

1. **IP adresa** = adresa síťového rozhraní (nikoli uzlu, ten jich může mít i několik). Používá se na síťové vrstvě a v současně používané verzi protokolu IPv4 je 32 bitová. Dnes je situace složitější o to, že se pro adresování postupně začíná zavádět adresování dle protokolu IPv6 (128 bitová adresa). O IPv6 si ale povíme dále.

2. **Port** = slouží v počítačových sítích při komunikaci pomocí protokolů TCP a UDP k rozlišení aplikace v rámci počítače. Je vázán na konkrétní transportní protokol (TCP nebo UDP), tj. stejné hodnoty portů, ale s rozdílným transportním protokolem jsou 2 různé přístupové body a nemají spolu nic společného. Máme 2 × 65 535 portů.

Spojení IP adresy a portu se nazývá **socket**, zapisuje se např.: 147.229.151.242:3526.

IP adresa se skládá z 2 částí (viz obrázek 1):



Obrázek 1. Struktura IP adresy

Jsou to abstraktní adresy používané pro sjednocení různých typů lokálních sítí a v konkrétní síti musí být přepočítány na fyzické adresy. Průběžné směrovače využívají pro směrování pouze adresu sítě, a až směrovač v cílové síti se rozhoduje podle 2. části adresy.

Adresy se zapisují pomocí 4 dekadických čísel oddělených tečkami, např. 147.229.195.12.

IP adresa musí být v rámci celého Internetu jedinečná. Pro koordinaci přidělování IP adres existuje hierarchická struktura autorit (správců), která zajišťuje jejich jedinečnost.

Bitové zastoupení adresy síťové a adresy uzlové v IP adrese není pevné, ale mění se, čímž lze definovat různý počet různě velkých sítí. Podle velikosti síťové a uzlové části adresy se prostor IP adres rozděluje do 5 tříd označených písmeny:

- **třída A**: se skládá z 7bitového identifikátoru sítě (bit nejvyššího řádu je vždy nastaven na 0) a 24bitového identifikátoru stanice.
- **třída B**: se skládá z 14bitového identifikátoru sítě (dva bity nejvyššího řádu jsou vždy nastaveny na 10) a 16bitového identifikátoru stanice.

- **třída C**: se skládá z 21bitového identifikátoru sítě (tři bity nejvyššího řádu jsou vždy nastaveny na 110) a 8bitového identifikátoru stanice.
- **třída D**: tento rozsah je vyhrazen pro adresy speciálního typu zvané multicast (čtyři bity nejvyššího řádu jsou vždy nastaveny na 1110).
- **třída E**: byla ponechána jako rezerva. Určena pro experimentální účely. (čtyři bity nejvyššího řádu jsou vždy nastaveny na 1111).

Třída	binární hodnota prvních bitů	rozsah adres (desítkově)	počet bitů identifikátoru sítě	počet bitů identifikátoru stanice	max. počet sítí	max. počet stanic*	maska třídy (desítkově)
A	0	0.0.0.0 – 127.255.255.255	8-1=7	24	2^7= 128	2^{24}-2= 16777214	255.0.0.0
B	10	128.0.0.0 – 191.255.255.255	16-2=14	16	2^{14}= 16384	2^{16}-2= 65534	255.255.0.0
C	110	192.0.0.0 – 223.255.255.255	24-3=21	8	2^{21}= 2097152	2^8-2= 254	255.255.255.0
D multicast	1110	224.0.0.0 – 239.255.255.255	–	–	–	–	–
E rezervovaná	1111	240.0.0.0 – 255.255.255.255	–	–	–	–	–

Obrázek 2. Vlastnosti jednotlivých tříd IPv4

- * Dvojku je nutno odečíst proto, že první adresa z každého síťového rozsahu určuje **adresu sítě** a poslední adresa každého rozsahu tzv. „všesměrový oběžník“ (broadcast) neboli **všesměrovou adresu**. Viz dále.

V těchto třídách **A – E,** existují speciální typy IPv4 adres, které mají definovaný účel použití a nelze je použít jinak. Příklady znázorňuje obrázek 3.

Typ adresy	Význam
0.0.0.0(b) (samé nuly)	Tento počítač na této síti.
0000000...XXXXX(b) (adresa sítě samé nuly)	Počítač XXXXX na této síti.
YYYYY…00000000(b) (adresa stanice samé nuly)	Adresa sítě YYYYYY.
YYYY…11111111(b) (jedničky místo adresy poč.)	Všeobecný oběžník pro síť YYYY (broadcast). Lze zaslat i na vzdálenou síť.
1111111…111111(b) (samé jedničky)	Všeobecný oběžník na lokální síti – je určen všem stanicím. Nelze zaslat na vzdálenou síť.
127.XXX.XXX.XXX(d)	Vyhrazené adresy pro softwarovou místní smyčku pro komunikaci v rámci jednoho počítače (loopback). Datagram zůstává v počítači.
169.254.XXX.XXX(d) Zpravidla 169.254.0.1 (d)	APIPA (Automatic Private IP Addressing) pokud rozhraní nedostane

	IP adresu od DHCP serveru, přidělí si ji z tohoto rozsahu samo.

Obrázek 3. Specifické IP adresy

Otázky, úkoly

- Zjisti z jakého rozsahu má IP adresu tvůj počítač.
- Zjsiti, co je to multicast.

Další zdroje ke studiu

- Informace o IP adresách http://www.samuraj-cz.com/clanek/tcpip-adresy-masky-subnety-a-vypocty/ nebo http://cs.wikipedia.org/wiki/IP_adresa
- Zjištění vlastní IP adresy http://www.mojeip.cz/

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí.* FEKT Vysokého učení technického v Brně, Brno 2006.

Použité obrázky

[1] Autorem obrázku je Vojtěch Novotný.

[2] Autorem obrázku je Vojtěch Novotný.

[3] Autorem obrázku je Vojtěch Novotný.

39. Privátní – neveřejné IP adresy

Z výše uvedených IP adres jsou některé rozsahy určeny pro privátní rozsahy. O adresy z tohoto rozsahu není potřeba žádat a můžeme je používat ve svých privátních sítích dle libosti. Tím pádem ale zde není zaručeno splnění výchozího pravidla použití IP adres – a to jedinečnost IP adresy v rámci Internetu. Proto komunikaci uzlů s těmito adresami nesmí nikdy propustit směrovač (router) do vnější sítě (internetu).

Případná komunikace uzlu s privátní adresou s ostatními uzly v Internetu se řeší pomocí mechanizmu NAT (Network Adress Translation).

V jednotlivých třídách byly vyčleněny pro privátní adresy tyto rozsahy:

A 10.0.0.0 – 10.255.255.255

B 172.16.0.0 – 172.31.255.255

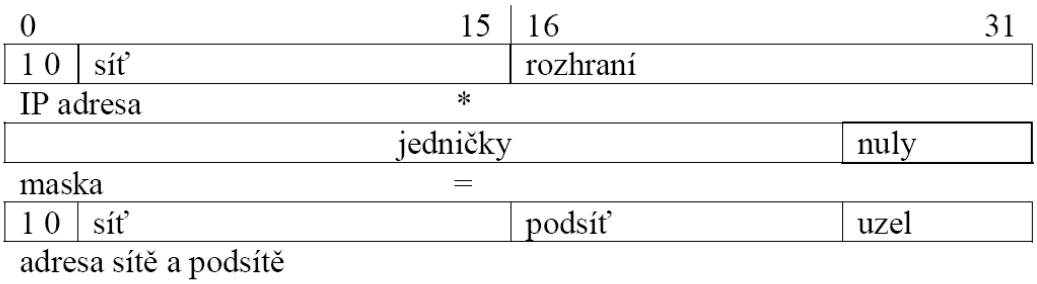
C 192.168.0.0 – 192.168.255.255

39.1 Podsíťování

Protože i rozdělení IP adresy na 2 části je dosti hrubé, což by vyžadovalo rozsáhlé směrovací tabulky v paměti směrovačů, byly zavedeny tzv. podsítě, kdy adresa síťového rozhraní byla dále rozdělena na 2 části:

- adresa podsítě (platí zde stejná omezení jako pro adresu sítě)
- adresa uzlu (rozhraní).

Jak velkou část která položka zabírá, definuje tzv. maska podsítě. Ta se skládá se souvislých posloupností jedniček a nul, kdy logickým součinem této masky s danou IP adresou získáme adresu podsítě (viz obrázek 1).



Obrázek 1. Výpočet adresy podsítě a adresy uzlu z IP adresy a masky podsítě

Příklad: Zařízení má IP adresu 203.105.92.107 a síťová maska je 255.255.255.192. Vynásobením adresy a masky získáme síťovou část adresy 203.105.92.64.

Adresa	203 11001011	105 01101001	92 01011100	107 01101011

Maska	255 11111111	255 11111111	255 11111111	192 11000000
Síťová část	203 11001011	105 01101001	92 01011100	64 01000000

Obrázek 2. Výpočet adresy podsítě a adresy uzlu z IP adresy a masky podsítě

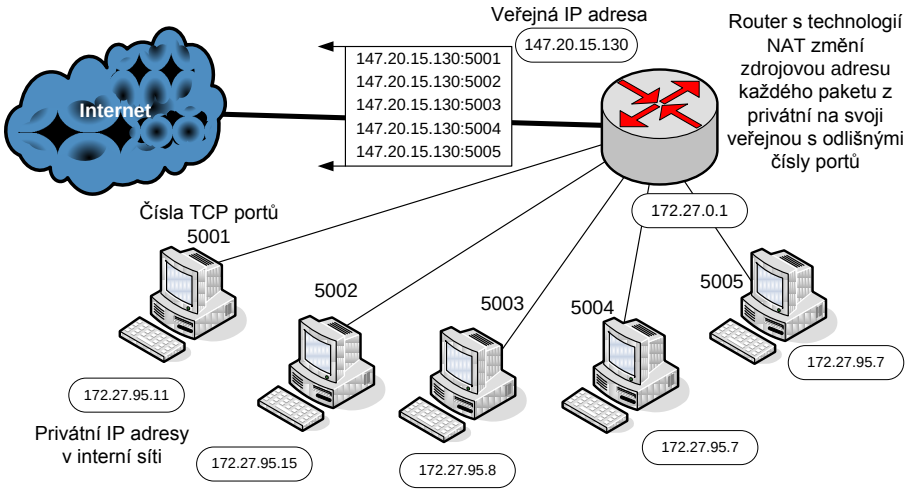
Tato maska je součástí směrovacích tabulek a využívá se až směrovači uvnitř cílové sítě.

39.2 Technika NAT (Network Adress Translation)

NAT – Network Adress Translation (překlad síťových adres) je funkce routeru, která překládá neveřejnou IP adresu z lokální sítě při přechodu dat do Internetu na IP adresu routeru. Pokud klient posílá data do Internetu právě přes směrovač s funkcí NAT, jeho adresa bude přeložena na veřejnou a pod náhodným portem uložena v tabulce překladů. Při odpovědi si router daný port vyhledá a pošle pakety na jemu přiřazenou IP adresu. Číslo portu je jednoznačné pro jeden překlad. Při nedoručení odpovědi se po stanovené době řádky tabulky vymažou.

Tato funkce šetří veřejné IP adresy a zvyšuje bezpečnost počítačů připojených za routerem. Z bezpečnostního hlediska dovoluje zakrýt před vnějším útočníkem strukturu sítě.

Existují dva režimy NAT: statický a dynamický. V statickém režimu se na rozdíl od dynamického umožní přístup pouze na vybrané privátní IP adresy.



Obrázek 3. Princip technologie NAT

Otázky, úkoly

- Sepiš výhody a nevýhody NATu
- Zkus z dvojice IP adresa-maska určit všechny možné síťové parametry.

Další zdroje ke studiu

- Informace o IP adresách http://www.samuraj-cz.com/clanek/tcpip-adresy-masky-subnety-a-vypocty/

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Porovn%C3%A1n%C3%AD_TCPIP_a_modelu_ISOOSI.jpg>.

[2] Autorem obrázku je Vojtěch Novotný.

[3] Autorem obrázku je Vojtěch Novotný.

40. Protokoly síťové vrstvy

Základním úkolem je přeprava paketů sítí pomocí na konkrétní síti nezávislého mechanismu. Hlavním protokolem je protokol IP. K němu jsou pak přidruženy další protokoly, ICMP a IGMP, ARP a RARP. Protokoly zajišťují:

- způsob na síti nezávislého adresování (IP adresy), převod IP adres na adresy používané v konkrétní síti (ARP) na úrovni síťového rozhraní, případně naopak pro zjištění IP adresy (RARP),
- formát datových jednotek pro jednotlivé protokoly (IP paket, jednotky ARP, RARP, ICMP a IGMP),
- směrování (podle směrových tabulek – statické, dynamické),
- pravidla přenosu paketů (fragmentace, doba života),
- testování přenosové cesty a řešení nestandardních situací (ICMP).

40.1 IP (Internet Protocol) protokol

IP (Internet Protocol) je hlavní protokol síťové vrstvy zajišťující přenos a směrování datových jednotek (paketů) intersítí.

Data se v IP síti posílají po blocích – paketech, které se nazývají datagramy. Jednotlivé datagramy putují sítí zcela nezávisle, na začátku komunikace není potřeba navazovat spojení či jinak „připravovat cestu“ datům, přestože spolu třeba příslušné stroje nikdy předtím nekomunikovaly. IP dále implementuje jednotné adresování (IP adresami).

IP v doručování datagramů poskytuje nespolehlivou službu, označuje se také jako best effort – „nejlepší úsilí“; tj. všechny stroje na trase se datagram snaží podle svých možností poslat blíže k cíli, ale nezaručují prakticky nic. Datagram vůbec nemusí dorazit, může být naopak doručen několikrát a neručí se ani za pořadí doručených paketů.

IP protokol nezajišťuje vlastní fyzický přenos, pouze předává paket k přenosu vrstvě síťového rozhraní.

IP paket:

Obrázek 1. Struktura IPv4 paketu

Popis jednotlivých polí:

- **verze IP**: v praxi se používá protokol verze 4 → $0100_{(b)}$,
- **délka záhlaví datagramu**: min. délka záhlaví je 20 B a maximální je 60 B,
- **typ služby (TOS)**: požadavky na parametry cesty (např. pro zajištění QoS),
- **délka celého datagramu**: maximální délka je 2^{16} = 65 536 B,
- **identifikace datagramu**: slouží k jednoznačné identifikaci případných fragmentů daného datagramu,
- **příznaky (volby)**: používají se k řízení fragmentace,
- **posunutí fragmentu**: slouží ke zpětnému poskládání datagramu z jednotlivých fragmentů,
- **doba života (TTL)**: dobu života určuje odesílatel. Každý směrovač při zpracovávání datagramu sníží tuto hodnotu o 1. V případě "zatoulání" datagramu v síti jej TTLtý směrovač zničí.
- **protokol vyšší vrstvy**: označuje, kterému protokolu přenášená data patří,
- **kontrolní součet**: kontrolní součet dat ze záhlaví (tj. nikoliv z dat za záhlavím datagramu). Pokud tento součet nesouhlasí, je datagram zničen. Každý směrovač musí vypočítávat nový kontrolní součet (minimálně kvůli změně hodnoty TTL).
- **IPv4 adresa odesílatele**
- **IPv4 adresa příjemce**
- **volitelné položky záhlaví**: prakticky se nepoužívají

Otázky, úkoly

Zjisti, zda-li existuje protokol IPv5?

Další zdroje ke studiu

- IP protokol na E-archivu http://www.earchiv.cz/a92/a248c110.php3.

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Ipv4-datagram.gif>.

41. IPv6

Internetový protokol verze 6 (IPv6) je následník IPv4, současné verze internetového protokolu, pro použití v Internetu.

Nejviditelnější změna, kterou přinesl IPv6, je daleko větší adresní prostor. IPv6 jsou 128 bitů dlouhé, oproti 32 bitům u IPv4. To umožňuje větší pružnost při přiřazování adres. Prodloužená délka adresy odstraňuje nepříjemnou potřebu použití překladu síťových adres (NAT). Není to však zdaleka jediná změna IPv6 implementuje celou řadu dalších nových mechanismů a specifikací, jako je objevování sousedů, automatická konfigurace, standardizovaná podpora bezpečnosti (podpora IPsec), podpora pro mobilní zařízení dočasně se nacházející mimo svou domácí síť, či funkce pro zajištění úrovně služeb (QoS).

Je běžné vidět příklady snažící se ukázat jak absurdně velký je adresní prostor IPv6. Obsahuje celkem 2^{128} (zhruba 3.4×10^{38}) adres, což odpovídá počtu 5×10^{28} adres pro každého z 6.5 miliardy dnes žijících lidí. Nebo také 2^{52} adres pro každou hvězdu ve známém vesmíru – milionkrát více adres pro každou hvězdu, než umožňoval protokol IPv4 pro naši planetu

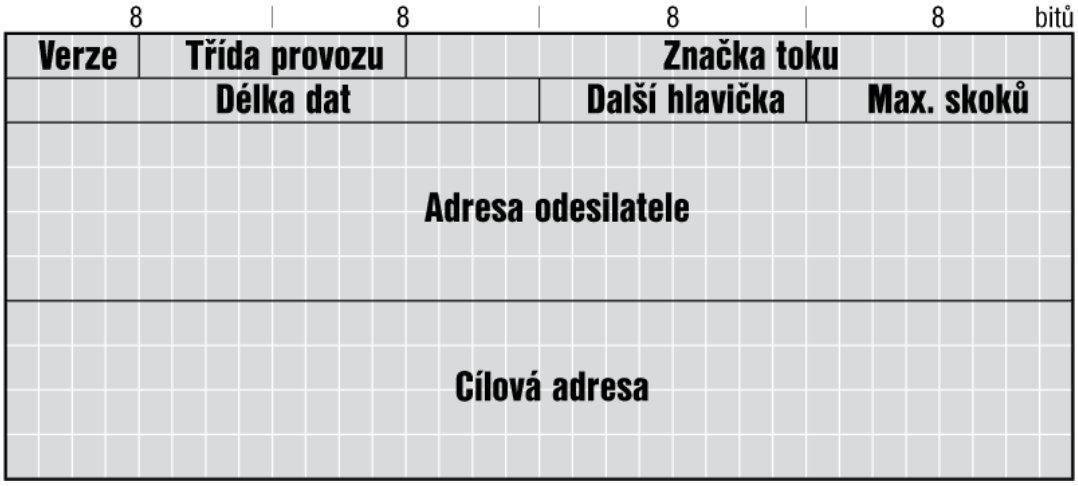
1.1.1.1 Notace - zápis

IPv6 adresy se zapisují jako osm skupin čtyř hexadecimálních číslic. Např. 2001:0db8:85a3:08d3:1319:8a2e:0370:7334 je platná adresa IPv6. Pokud je jedna nebo více ze čtyřčlenných skupin 0000, nuly mohou být vynechány a nahrazeny dvěma dvojtečkami (::). Např. 2001:0db8:0000:0000:0000:0000:1428:57ab lze nahradit 2001:0db8::1428:57ab. Libovolný počet po sobě následujících skupin 0000 může být nahrazen dvěma dvojtečkami, pokud se v adrese toto nahrazení vyskytuje pouze jednou. Předcházející nuly ve skupině mohou být také nahrazeny (jako v ::1 pro místní smyčku). Adresy níže jsou tedy platné, rovnocenné a stejné:

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

1.1.1.2 IPv6 paket

Paket IPv6 se skládá ze dvou hlavních částí: hlavičky a těla. Hlavička se nachází v prvních 40 oktetech (320 bitů) paketu a obsahuje:



Obrázek 1. Struktura IPv6 paketu

- **Verzi** — 4 bity, verze 6.
- **Dopravní třídu** — 8 bitů na prioritu paketu.
- **Pojmenování toku** — 20 bitů pro správu QoS. Původně určeno pro speciální obsluhu aplikací reálného času, nyní se nepoužívá.
- **Délka těla** — 16 bitů pro délku těla paketu (max. 64 kB). Při vynulování se nastaví „jumbo“ tělo (max. 4 GB).
- **Následující hlavička** — 8 bitů, určuje další vnořený protokol. Hodnoty se shodují s hodnotami definovanými pro IPv4.
- **Zdrojová a cílová adresa** — 128 bitů na každou adresu.
- **Hop Limit** – obdoba TTL (životnost paketu).

Otázky, úkoly

- Porovnej hlavičky IPv4 a IPv6 protokolu.
- Zjisti, jaký je dnes poměr využití IP a IPv6.

Další zdroje ke studiu

- České stránky o IPv6 https://www.ipv6.cz/
- IPv6 na Wikipedii http://cs.wikipedia.org/wiki/IPv6

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

Použité obrázky

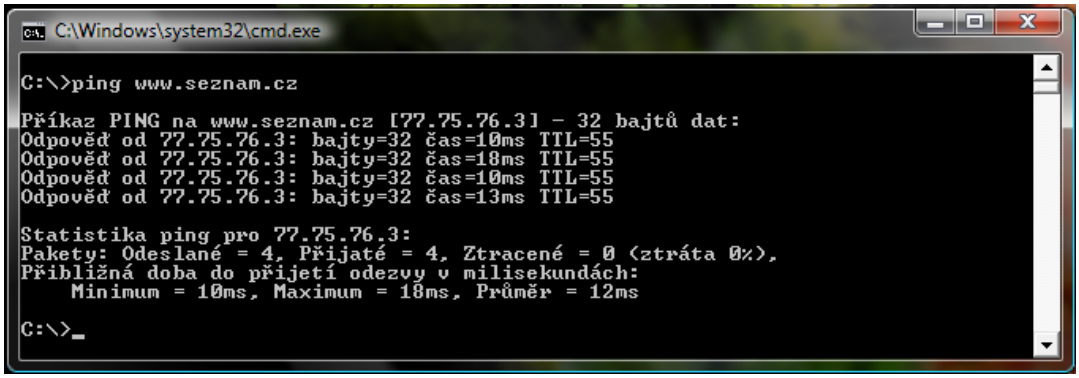
[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Ipv6-datagram.gif>.

42. ICMP, DHCP

42.1 ICMP (Internet Control Message Protocol)

ICMP doplňuje činnost protokolu IP o přenos řídicích zpráv mezi směrovači navzájem nebo mezi směrovači a koncovými uzly (počítači). Tento protokol se používá pro:

- testování dosažitelnosti cílového uzlu prostřednictvím protokolu IP (např. příkazem PING),
- chybové zprávy – nedosažitelnost adresáta, vypršení doby života, chybný parametr v záhlaví paketu, apod.,
- synchronizace času a odhad doby přenosu,
- řízení přenosu – upozornění na zahlcení mezilehlého nebo koncového uzlu,
- přesměrování trasy – upozornění hosta směrovačem, že existuje vhodnější brána k danému cíli,
- získání přídavných informací – např. síťové části IP adresy (zastaralé).



Obrázek 1. Výstup příkazu ping v prostředí Windows Vista

42.2 Protokol DHCP (Dynamic Host Configuration Protocol)

DHCP protokol umožňuje prostřednictvím DHCP serveru nastavit všem stanicím sadu parametrů nutných pro komunikaci v sítích používajících rodinu protokolů TCP/IP včetně parametrů doplňujících a uživatelsky definovaných (IP adresa, maska sítě, výchozí brána, adresy DNS serverů, a další údaje). Významným způsobem tak zjednodušuje a centralizuje správu počítačové sítě.

Klienti žádají server o IP adresu, ten u každého klienta eviduje půjčenou IP adresu a čas, do kdy ji klient smí používat (doba zapůjčení). Poté co vyprší, smí server adresu přidělovat jiným klientům.

DHCP transakce

- *A→všem*: Kdo jsem? Mám Eth 00:8C:16:A2:31:06. (DHCPDiscovery)
- *DHCP server→A*: Mohu nabídnout 1.2.16.8. (DHCPOffer)

- *A→DHCP server*: Prosím 1.2.16.8. (DHCPRequest)
- *DHCP server→A*: Je tvá a takováto jsou další nastavení. (DHCPAcknowledge)
- Aresa je „pronajata“ na omezenou dobu, klient musí před uplynutím doby zapůjčení z DHCPAcknowledge obnovit svou IP adresu. Pokud lhůta uplyne, aniž by dostal nové potvrzení, klient musí IP adresu přestat používat.

DHCP protokol nemá žádné bezpečnostní mechanismy a tak

- útočník může v síti nainstalovat vlastní DHCP server, který bude klientům vysílat neplatné údaje (útok DoS) nebo je bude směrovat na vlastní směrovač (útok na důvěrnost/integritu),
- útočníkův počítač může postupně vystupovat jako více klientských počítačů a svými žádostmi tak může vyčerpat přidělený počet IP adres (útok DoS).

Otázky, úkoly

- Vyzkoušej si práci s ICMP pomocí příkazů traceroute a ping v příkazovém řádku.
- Zjisti, zda-li tvůj počítač využívá služeb DHCP serveru. Jak by jsi tuto službu zapnul.
- Kde se v domácí síti nejčastěji nachází DHCP server?

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

Použité obrázky

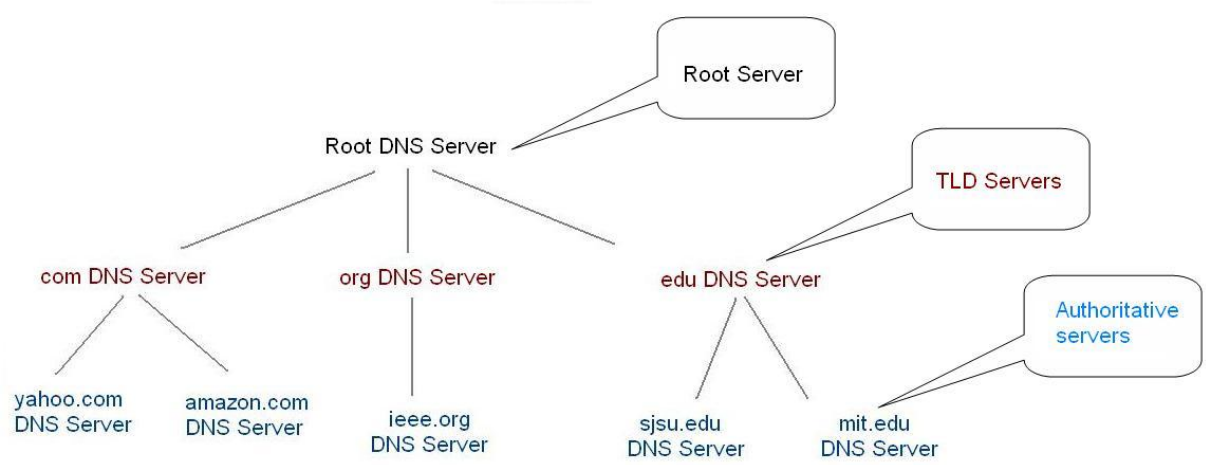
[1] Autorem obrázku je Vojtěch Novotný.

43. Jmenný systém – DNS protokol

V síti TCP/IP se adresuje podle IP adresy, což je nějaké číslo. Zapamatovat si byť jen několik IP adres je problematické. Pro lidi je přirozenější pracovat se jmény, tedy s řetězcovým označením cíle komunikace. Vzniká tu tedy problém mapování jméno–IP adresa. Řešením jede centralizovaný systém jmen s hierarchickou strukturou DNS (Domain Name System), který zajišťuje převod jmen na IP adresy a naopak. Je to systém založený na modelu klient-server.

Kořenové jmenné servery představují zásadní část technické infrastruktury Internetu, na které závisí spolehlivost, správnost a bezpečnost operací na internetu. Dalo by se říci, že jsou srdcem internetu. Představují jedno z mála jeho zranitelných míst. Tyto servery (je jich přibližně 13 po rozmístěných po celém světě) poskytují DNS informace ostatním DNS serverům. Jsou součástí DNS, celosvětově distribuované databáze, která slouží k překladu unikátních doménových jmen na ostatní identifikátory.

Vztah mezi IP adresou a jménem je velmi volný, takže doména není svázána s určitou sítí. Dále platí, že jedno jméno může být použito pro více IP adres (např. pro směrovač). Opačně pro jednu IP adresu může existovat více jmen, rozlišující nejčastěji typy služeb, které jsou uzlem poskytovány, např. www, ftp, apod. Jedno z těchto jmen však musí být to pravé (kanonické) a ostatní jsou přezdívky.



Obrázek 2. Struktura systému doménových jmen

DNS odpovědi lze podvrhnout různými formami útoků, proto byl zaveden DNSSEC, který umožňuje:

- ověřit platnost odpovědi (elektronický podpis)
- ověřit neexistenci daného záznamu

DNSSEC má ovšem problémy s prosazováním.

Národní znaky v názvu domény

- klasické DNS je omezeno na (podmnožinu) ASCII, nelze tedy používat různé specifické „národní“ znaky. Existoval však tlak (zejména od asijských zemí) na zavedení národních abeced.
- Byl zaveden standard Internationalized Domain Names (IDN)
  - implementováno v klientech, servery beze změny
  - mapováním se zmenší počet variant
  - zakóduje se do ASCII a přidá předpona xn--
  - např. blahopřání převede na: xn--blahopn-mwa3iv2c
  - první zavedl Hong Kong (1999)
  - ČR – CZ.NIC provedl (opakovaně) průzkum mezi uživateli, o zavedení IDN není zájem (2012).

Otázky, úkoly

- Zjisti jaký je stav zavedení národních znaků v názvech domény v ČR.

Další zdroje ke studiu

- Článek o DNS od Jiřího Peterky http://www.earchiv.cz/a98/a816k180.php3

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-02-14]. Dostupný pod licencí Public domain na WWW: < http://en.wikibooks.org/wiki/File:Strucutre-of-dns.jpg>.

44. Směrovací protokoly síťové vrstvy

O směrování se v síti TCP/IP starají směrovače, které směřují pakety na základě směrovacích tabulek. Směrování může být, jak již bylo řečeno, řešeno staticky nebo dynamicky. U dynamického směrování jsou výměny zajišťovány směrovacími protokoly. V současnosti jsou to v síti TCP/IP protokoly RIP a OSPF.

44.1 Směrovací protokol RIP (Routing Information Protocol)

Směrovací protokol RIP (RIPv2) si jako měřítko dosažitelnosti sítě se bere počet mezilehlých směrovačů a maximální vzdálenost je 15. Směrovače posílají své směrovací tabulky sousedním směrovačům každých 30 s. Pro přenos tabulek se využívá transportní protokol UDP. Základním kriteriem dosažitelnosti sítě je vzdálenost k této síti. Vzdálenost je vyjádřena jako počet mezilehlých směrovačů mezi daným směrovačem a cílovou sítí (hop count). Již se ale nijak nezohledňuje propustnost linek, tedy jejich rychlost, maximální velikost přepravovaných rámců, apod.

K dané cíli z daného směrovače vede pouze jediná cesta. Nelze tedy využít možnosti rozložení zátěže mezi více stejně dlouhých cest. Je-li vzdálenost rovna 16, je síť chápána jako nedosažitelná. Rozšíření informace o změně mezi ostatní směrovače je dosti pomalá. Další nevýhodou je značné zatížení sítě, neboť si směrovače posílají celé tabulky, jejichž velikost závisí na celkovém počtu sítí.

Činnost směrovače s RIP

- každých 30 s pošle směrovací tabulku sousedům
- maximální vzdálenost je 15
- soused přičte ke vzdálenostem 1 a porovná se svou tabulkou, změní svůj záznam pokud:
  - cíl ještě neznal
  - znal k cíli delší cestu
  - cesta k cíli vede přes odesilatele tabulky (aktuálně používaná cesta se zhoršila)

44.2 Směrovací protokol OSPF (Open Shortest Path First)

Směrovací protokol OSPF je složitější, ale dokonalejší než protokol RIP. Umožňuje lépe využít nabízených kapacit sítě, rychleji reagovat na změny v síti. Každý směrovač si shromažďuje informace o topologii celé oblasti. Směrovače si předávají informace o stavu přímých linek. Stav linek lépe odpovídá skutečné propustnosti sítě. Na základě stavů linek se pomocí Dijkstrova algoritmu vypočítá nejkratší cesta (s nejnižší cenou). V případě změny v síti se tato změna záplavovým mechanismem rozšíří velmi rychle po celé oblasti. Tento protokol

také umožňuje rozdělit zatížení na více cest, existuje-li více cest se stejnou cenou. OSPF má menší režii než RIP (informace se posílají každých 30 minut) a je lépe škálovatelný, tj. jeho režie s růstem celé soustavy sítí neroste tak rychle, jak by rostla v případě protokolu RIP.

Metrika protokolu OSPF není omezena hodnotou 16 jako u protokolu RIP. Může nabývat hodnotu až 65 535.

Činnost směrovače s OSPF

- založeno na stavu linek – všechny směrovače si vyměňují informace
- maximální metrika 65 535
- všechny směrovače ve stejné oblasti udržují totožnou mapu sítě
- každou změnu okamžitě hlásí sousedům
  - šíří se roztékáním – změna se předává všem ostatním
  - pozná opakovanou aktualizaci (cyklus), neposílá dál
- z mapy sítě vypočítá nejkratší cesty ke všem cílům

Otázky, úkoly

- Porovnej v tabulce výhody a nevýhody RIP a OSPF.

Další zdroje ke studiu

- Popis OSPF http://www.cs.vsb.cz/grygarek/SPS/lect/OSPF/ospf.html

Použité zdroje

[1] Wikipedie: Otevřená encyklopedie: Routing Information Protocol [online]. c2012 [citováno 24. 08. 2012]. Dostupný z WWW: <http://cs.wikipedia.org/w/index.php?title=Routing_Information_Protocol&oldid=8934388>

[2] Wikipedie: Otevřená encyklopedie: Open Shortest Path First [online]. c2012 [citováno 24. 08. 2012]. Dostupný z WWW: <http://cs.wikipedia.org/w/index.php?title=Open_Shortest_Path_First&oldid=8570904>

45. Transportní protokoly

Na transportní vrstvě existují 2 protokoly: TCP a UDP. Úkolem transportního protokolu je hlavně multiplex a demultiplex datových toků od jednotlivých procesů, které komunikují s transportní vrstvou přes speciální přístupové body, tzv. porty. Jsou to místa v paměti, kterým je přiděleno 16bitové číslo. Přitom stejné číslo může být přiděleno portu TCP a UDP. Označuje to však dva různé porty (maximálně tedy existuje 2 × 65 535 portů).

Protokoly UDP a TCP jsou využívány odlišnými aplikacemi. Protokol TCP je podstatně složitější než UDP, neboť nabízí více funkcí. Každý z nich nabízí různé služby.

45.1 Protokol TCP (Transmission Control Protocol)

TCP – Zajišťuje přenos dat se zárukami, který vyžadují aplikace, kde nesmí „chybět ani paket“. Jedná se o přenosy souborů, e-mailů, WWW stránek atd. Záruka se vztahuje na řešení ztrát přenášených paketů, zachování jejich pořadí a odstranění duplikace.

TCP poskytuje:

spojově orientovanou službu - komunikace probíhá ve 3 fázích: navázání spojení, vlastní přenos dat, rozpad spojení. Znamená to tedy, že při požadavku na komunikaci se nejprve vytvoří spojení, přes toto spojení jsou následně odesílána veškerá data.

spolehlivou službu (tzv. bitová roura) – pomocí pořadových čísel, délky TCP segmentu, kontrolního součtu, časovače odpovědi a kladného potvrzování. Potvrzení posílá přijímač po příjmu paketu. Chyba je indikována v případě, kdy potvrzení nepřijde do časového limitu vůbec anebo 3krát po sobě přijde potvrzení se stejnou hodnotou pořadového čísla přijatého bajtu. Pak následuje procedura opakování. Příjemce si segmenty přišlé mimo pořadí uchovává, a je-li tedy přijat znovuvyslaný chybějící segment, pak se v potvrzení potvrdí všechna přijatá data tvořící souvislý tok bajtů. Není tedy třeba vysílat vše od původně ztraceného segmentu.

<table>
<tr><th>Bity</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>0</td><td colspan="16">zdrojový port</td><td colspan="16">cílový port</td></tr>
<tr><td>32</td><td colspan="32">číslo sekvence</td></tr>
<tr><td>64</td><td colspan="32">potvrzený bajt</td></tr>
<tr><td>96</td><td colspan="4">offset dat</td><td colspan="6">rezervováno</td><td colspan="6">příznaky</td><td colspan="16">okénko</td></tr>
<tr><td>128</td><td colspan="16">kontrolní součet</td><td colspan="16">Urgent Pointer</td></tr>
<tr><td>160</td><td colspan="32">volby (volitelné)</td></tr>
</table>

192	volby (pokračování)	výplň (do 32)
224	data	

Obrázek 1. Struktura TCP

45.2 Protokol UDP (User Datagram Protocol)

Protokol UDP zajišťuje minimální nástavbu nad protokol IP. Na rozdíl od TCP nabízí nespojovanou a nespolehlivou službu, což umožňuje, aby byl rychlejší, neboť vyžaduje minimum režie. Případné zabezpečení si musí zajistit aplikace sama.

UDP poskytuje službu:

- **nespojově orientovanou** – pakety se vysílají příjemci bez ověření existence, dostupnosti a připravenosti cíle. Neexistuje potvrzování přijetí ani řízení toku dat.
- **nespolehlivou** – UDP neřeší zabezpečení dat během přenosu, ani detekci a korekci případně vzniklých chyb.

UDP – Zajišťuje přenos dat bez záruk, který využívají aplikace, u kterých by bylo na obtíž zdržení v síti způsobené čekáním na přenos všech paketů a ztráty se dají řešit jiným způsobem (např. snížení kvality, opakování dotazu). UDP se uplatní všude tam, kde potřebujeme co nejjednodušší implementaci a také všude tam, kde potřebujeme data co nejrychleji. Například dojde-li při real-time přenosu hlasu k výpadku několika paketů jsou již případné korekce zbytečné. Lidský mozek si poradí s vypadnutím několika hlásek z rozhovoru lépe, než kdyby se mělo čekat, až se přesně sestaví celá zpráva. Využívá se pro DNS, VoIP, streamované video, internetová rádia, vyhledávání sdílených souborů v rámci sítě DC++, on-line hry atp.

+	bity 0 - 15	16 - 31
0	zdrojový port	cílový port
32	délka	kontrolní součet
64	data	

Obrázek 2. Struktura UDP

Otázky, úkoly

- Porovnej v tabulce výhody a nevýhody TCP a UDP.

Další zdroje ke studiu

- Seznam obvykle používaných portů http://cs.wikipedia.org/wiki/Seznam_%C4%8D%C3%ADsel_port%C5%AF_TCP_a_UDP

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

Použité obrázky

[1] Autorem je Vojtěch Novotný

[2] Autorem je Vojtěch Novotný

46. APLIKAČNÍ PROTOKOLY

46.1 Protokol HTTP (Hypertext Transfer Protocol)

HTTP je internetový protokol určený původně pro výměnu hypertextových dokumentů ve formátu HTML.

V současné době je používán i pro přenos dalších informací. Pomocí rozšíření MIME, umí HTTP přenášet jakýkoli soubor (podobně jako e-mail), používá se společně s formátem XML pro tzv. webové služby (spouštění vzdálených aplikací).

Protokol funguje způsobem dotaz-odpověď. Uživatel (pomocí programu, obvykle internetového prohlížeče) pošle serveru dotaz ve formě čistého textu (obvykle na port TCP/80), obsahujícího označení požadovaného dokumentu, informace o schopnostech prohlížeče apod. Server poté odpoví pomocí několika řádků textu popisujících výsledek dotazu (zda se dokument podařilo najít, jakého typu dokument je atd.), za kterými následují data samotného požadovaného dokumentu.

Pokud uživatel bude mít po chvíli další dotaz na stejný server (např. proto, že uživatel v dokumentu kliknul na hypertextový odkaz), bude se jednat o další, nezávislý dotaz a odpověď. Z hlediska serveru nelze poznat, jestli tento druhý dotaz jakkoli souvisí s předchozím. Kvůli této vlastnosti se protokolu HTTP říká bezestavový protokol – protokol neumí uchovávat stav komunikace, dotazy spolu nemají souvislost. Tato vlastnost je nepříjemná pro implementaci složitějších procesů přes HTTP (např. internetový obchod potřebuje uchovávat informaci o identitě zákazníka, o obsahu jeho „nákupního košíku“ apod.). K tomuto účelu byl protokol HTTP rozšířen o tzv. HTTP cookies, které umožňují serveru uchovávat si informace o stavu spojení na počítači uživatele.

K protokolu HTTP existuje také jeho bezpečnější verze HTTPS (port 443), která umožňuje přenášená data šifrovat a tím chránit před zneužitím.

46.2 Protokol FTP (File Transfer Protocol)

Protokol FTP řeší problematiku obousměrného přenosu datových souborů mezi dvěma počítači.

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.

FTP běžně pracuje na dvou portech, 21 a 20 a běží výhradně přes TCP. FTP server naslouchá na portu 21 na příchozí spojení z FTP klienta. Na tomto portu

běží příkazy, které zachytává server. Na portu 20 se přenáší pouze data, nikoliv příkazy.

Samotný přenos, včetně odeslání hesla, není šifrován, je tedy považován za nebezpečný. Existuje proto několik zabezpečených nástupců (SCP, FTPS, SFTP,…).

46.3 Elektronická pošta (e-mail)

SMTP (Simple Mail Transfer Protocol) protokol

Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem; zpráva je doručena do tzv. poštovní schránky adresáta, ke které potom může uživatel kdykoli (off-line) přistupovat (vybírat zprávy) pomocí protokolů POP3 nebo IMAP. Jedná se o jednu z nejstarších aplikací, původní norma byla vydána v roce 1982. Původně měl obsah elektronické pošty textovou povahu, dnes se používá i pro přenos multimediálních dokumentů.

E-mailová komunikace je založena na bázi server/klient

- Poštovní server (MTA) (SMTP server) očekává požadavky na portu č. 25.
- Poštovní klient je program, který zajišťuje odesílání zpráv a vybírání schránek. Příkladem je např. Microsoft Outlook, Mozilla Thunderbird a další. Je to specializovaný editor, který umí kromě vytvoření zprávy také manipulovat se schránkami, odeslat zprávu SMTP protokolem nejbližšímu MTA a převzít zprávu ze serveru prostřednictvím POP3 nebo IMAP.
- Vlastním doručováním zprávy po síti až k adresátovi se klient nezabývá.

POP3 (Post Office Protocol verze 3) protokol

POP3 protokol je určen k jednoduchému a rychlému stahování pošty ze vzdáleného úložiště na počítač, který nemusí být nutně nepřetržitě připojen k internetu. Protokol POP3 má pro své účely vyhrazen TCP port 110. Komunikace probíhá v střídajících se výměnách mezi klientem a serverem.

Protokol IMAP (Internet Message Access Protocol)

Protokol IMAP je na rozdíl od protokolu POP3 mnohem složitější a nabízí mnohem větší komfort pro práci se zprávami. IMAP protokol je optimalizován pro práci s poštou v režimu dlouhodobého připojení. Na rozdíl od protokolu POP, kde se zprávy stahují okamžitě ze serveru do klientského počítače, jsou zprávy stále uloženy na serveru.

Snad nejdůležitější rozdíl od POP3 je možnost práce se zprávami na straně serveru. Klient může zprávy přesouvat mezi schránkami, editovat zprávy, ukládat, načítat. Protokol IMAP je optimalizován pro práci s mobilními zařízeními. Umožňuje selektivní načítání emailových zpráv, nebo dokonce jejich

částí. Tato vlastnost je nedocenitelná při přístupu k poštovní schránce po pomalé telefonní lince (například z mobilního telefonu).

Otázky, úkoly

- Co jsou to cookies?
- Najdi adresu nějakého FTP serveru.
- Vyzkoušej si připojení na FTP server.

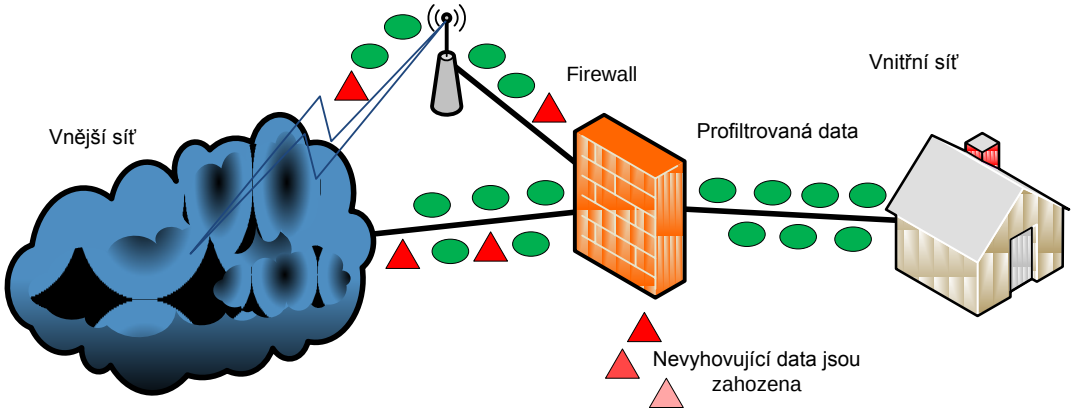
Další zdroje ke studiu

Použité zdroje

[1] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

47. Bezpečnost TCP – firewally

Firewally jsou zařízení určená k ochraně před různými typy útoků metodou filtrování přenášené komunikace. K filtraci přenášené komunikace případného útočníka se využívá především síťová, transportní a aplikační vrstva.



Obrázek 1. Princip činnosti firewallu

47.1 Paketové filtry

(Packet Filters): síťová a transportní vrstva, založen na pravidlech stanovených pro dvojici zdrojová IP adresa a cílová IP adresa + určení portů, filtrace je prováděna tak že se nejprve zjistí zdrojová i cílová adresa a porty, a v tabulce pravidel se hledá pravidlo, kterému daná dvojice vyhovuje, zde mohou nastat tři případy:

- allow – povolení průchodu
- deny – zamítnutí a odeslání chybového hlášení
- discard – zamítnutí bez hlášení (útočník se nedozví ani o existenci systému)

Je vhodné nastavit taková pravidla taková, aby zařízení z vnější sítě nemohla komunikovat přímo s firewallem, nebo se vydávat za firewall. Po projití celé tabulky bývá zvykem nastavení pravidla k zamítnutí všech ostatních paketů.

Problém této strategie je ale v tom, že je poměrně snadné falšovat údaje o původu paketu (o síti a uzlu, ze kterého přichází). Stejně tak tato metoda nemusí postačovat pro rozpoznání některých potenciálních útoků.

Výhoda - vysoká propustnost, nevýhoda - útoky přes protokoly vyšších vrstev.

Příklad filtračních pravidel pro lokální síť s adresou 192.168.1.0:

	zdrojová adresa	zdroj. port	cílová adresa	cílový port	akce	popis
1	any	any	192.168.1.0	>1023	allow	příjem reakcí na výzvy zevnitř
2	192.168.1.1	any	any	any	deny	nelze zneužít adresu firewalu
3	any	any	192.168.1.1	any	deny	blokování spojení s firewalem
4	192.168.1.0	any	any	any	allow	povolení komunikace zevnitř
5	any	any	192.168.1.2	SMTP	allow	příjem e-mailů zvenku
6	any	any	192.168.1.3	HTTP	allow	přístup na web zvenku
7	any	any	any	any	deny	všechno ostatní nepustit

Postup paketového filtru:

1) zjištění zdrojové i cílové IP adresy a portů.

2) průchod tabulkou po jednotlivých řádcích odshora, dokud není nalezen řádek, který odpovídá danému paketu.

3) Provede akci uvedenou v příslušném řádku:

- propustí („allow“),
- zničí a odesílateli zašle chybové hlášení („deny“),
- zničí a žádné chybové hlášení nezasílá („discard“).

- První řádek tabulky zajišťuje navázání TCP spojení iniciovaných z vlastní sítě. (Pozn: Iniciátor TCP spojení vždy stanovuje přijímací port větší než 1023.)
- Druhý řádek zabraňuje útočníkovi vystupovat v síti jako firewal.
- Třetí řádek zabraňuje vnějšímu útočníkovi komunikovat s firewalem.
- Čtvrtý řádek umožňuje všem prvkům sítě komunikovat s kýmkoliv z vnější sítě a použít přitom jakýkoliv protokol.
- Pátý řádek umožňuje projít všem paketům z vnější sítě, pokud nesou data protokolu SMTP („Simple Mail Transport Protocol“ – tj. email)
- Šestý řádek umožňuje projít všem paketům z vnější sítě, pokud nesou data protokolu HTTP („HyperText Transfer Protocol“ – tj. web).
- Poslední řádek je velmi důležitý – vše co nespadá pod výše uvedená pravidla nepustit.

47.2 Firewally se stavovou inspekcí

(Stateful Inspection Firewalls nebo Circuit Level Firewalls): transportní vrstva, tyto firewally využívají mimo adresy a portu také informaci o stavu spojení funguje tak, že je zaznamenán paket a je očekávána příslušná odezva, do vnitřní sítě se tak dostanou pouze pakety reagující na výzvu právě z vnitřní sítě. Paket je propuštěn do vnitřní sítě, pouze pokud splňuje očekávané parametry. Do

vnitřní sítě se tak zvenčí dostanou pouze pakety z komunikace iniciované vnitřním prvkem sítě.

Mnohé útoky lze dnes rozpoznat až tehdy, když si firewally začínají všímat také vzájemných souvislostí a vztahů, a dokáží si dát "dvě a dvě dohromady". Například když si dokáží uvědomit, že najednou přichází výrazně vyšší množství individuálních požadavků než je obvyklé, což vyvolává náhlé zahlcení toho, kdo má tyto požadavky vyřizovat. Důsledkem může být až úplná nedostupnost konkrétní služby. To je princip dnes tolik oblíbených útoků typu DoS (Denial of Service), které navíc mohou být i různě distribuované (když požadavky způsobující zahlcení přichází z různých zdrojů, jednajících ve vzájemné součinnosti).

47.3 Proxy firewally

(Proxy Firewall): aplikační vrstva, vzhledem k práci na aplikační vrstvě umí přiřadit data paketů aplikačním protokolům, posoudit nestandardní parametry, často umožňují i možnost autentizace odesílatele což zabraňuje útočníkovy klamat pomocí modifikace IP adresy, varianta SSLproxy.

Pokud firewall "vidí" až na aplikační vrstvu a detailně rozumí tomu, co se zde odehrává, podle jakých pravidel atd. je schopen se nejlépe rozhodnout o legitimnosti dat. Bez této schopnosti jsou firewally bezbranné vůči celé řadě "moderních" a čím dál tím častějších útoků, jakými jsou například útoky červů (např. Slammer, Code Red či Nimda), útoky pomocí skriptů (cross-site scripting), vůči emailovému bombardování (mail bombing) atd.

- (+) nelze vést útok přes protokoly vyšší vrstvy, (-) nízká propustnost.

Moderní firewally poskytují i nové funkce, jako je například antivirová filtrace přenášených dat, filtrace spamu apod.

47.4 Umístění firewalů

- Paketové filtry a firewaly se stavovou inspekcí: na hranici vnitřní a vnější sítě.
- Proxy firewaly: za firewaly paketové/transportní vrstvy. Zpravidla jich je více a podle typů protokolů v aplikační vrstvě (vyšší propustnost), mohou běžet jako aplikace v koncovém zařízení.
- Moderní firewaly poskytují i nové funkce, jako je například antivirová filtrace přenášených dat, filtrace spamu apod.

47.5 Demilitarizovaná zóna (DMZ)

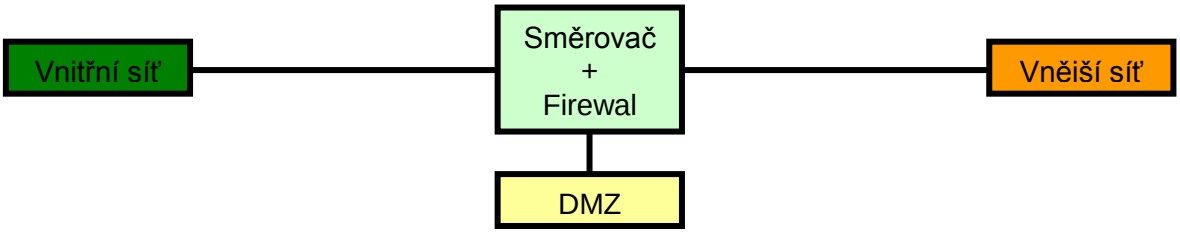
Demilitarizovaná zóna (DMZ): část sítě, ve které je filtrována komunikace jak z vnější, tak i z vnitřní sítě.

Do DMZ se umisťují servery, které jsou tak filtračními pravidly chráněny jak před útoky z vnější sítě, tak i před útoky z vnitřní sítě.

Realizace:

a) dva firewaly

b) směrovač s filtrací.



Otázky, úkoly

- Používáš / nepoužíváš firewall? Proč tomu tak je?
- Vymysli, proti jakým útokům firewall neochrání.

Další zdroje ke studiu

- Firewally na Wikipedii http://cs.wikipedia.org/wiki/Firewall

Použité zdroje

[1] BURDA, Karel, doc. Ing. CSc. *Návrh, správa a bezpečnost počítačových sítí*. FEKT VUT v Brně, Brno 2007.

Použité obrázky

[1] Autorem obrázků je Vojtěch Novotný.

48. Volba bezpečného hesla

V souvislosti s velkou spoustou služeb, které využívají informační systémy, se často setkáte se zabezpečením přístupu pomocí hesla. Systém může být jakkoliv bezpečný, ale pokud máte slabé heslo, tak je pro útočníka hračkou se do systému dostat. Za bezpečné heslo je považováno takové, které není snadno zjistitelné nebo uhodnutelné.

Heslo by nemělo vzniknout z nějakého údaje o nás či našem okolí, například:

- jméno někoho z rodiny či vlastní jméno, jméno psa, apod.
- č. domu, adresa, telefonní číslo…
- hesla typu: heslo, 1234, 1111,…
- rodné číslo či datum narození

Nejbezpečnější hesla jsou tedy „nesmyslné“ kombinace znaků. Bohužel o to hůře si ale heslo zapamatujeme i my sami, a pokud ho pravidelně nepoužíváme, brzy ho zapomeneme. A napsat si heslo někde na papírek není vůbec dobrý nápad. Vhodnější je vymyslet si k heslu nějakou mnemotechnickou pomůcku, podle které si ho snáze zapamatujeme (tato pomůcka ovšem musí zůstat stejně tajná jako heslo samotné).

48.1 Délka hesla

Mohlo by nás mylně napadnout, že PIN kreditní karty jsou pouze čtyři číslice, a proto by čtyři obyčejné znaky mohly stačit. Nezapomínejme ale, že v případě kreditní karty máme ještě omezený počet chybných zadání hesla (PINu) a pokud několikrát zadáme chybné heslo, karta se nám zablokuje. Ale toto zabezpečení mají jen málokteré jiné systémy, proto čtyři obyčejné znaky většinou zdaleka nestačí. Délka bezpečného hesla se také postupně prodlužuje díky síle výpočetních systémů.

48.2 Použité znaky

V dobrém hesle by neměly být použité jen běžné znaky. Čím větší množinu znaků v hesle použijeme, tím je složitější heslo prolomit.

K dispozici máme 10 číslic, 26 základních písmen abecedy (a-z), které můžeme zdvojnásobit použitím velkých a malých písmen, dále můžeme přidat znaky s diakritikou a nakonec i interpunkční znaménka (. , : ; - ? ! ...) a spoustu speciálních znaků (& @ # $ ^ _ * ...). Dohromady tedy máme k dispozici přes 80 znaků relativně snadno použitelných na běžné klávesnici.

Některé servery ovšem nepodporují použití určitých speciálních znaků (např. $, \, /, ', <, >, ", & , ˇ) z bezpečnostních důvodů.

48.3 Kvalita hesla

V tabulce vidíte kolik různých kombinací dané délky lze utvořit z různého počtu použitelných znaků. Pro představu je i každého údaje napsán i přibližný čas potřebný k vyzkoušení všech možných kombinací vhodným softwarem, který je schopen vyzkoušet 100 kombinací za sekundu. Není ale vyloučeno, že útočník nemůže použít více strojů počítačů, které budou na prolamování hesla pracovat najednou, a tedy se o čas podělí. Také ale můžeme vzít v úvahu, že lepší programy na prolomení hesla, které nejprve zkoušejí slova a teprve postupně přechází ke složitějším a nesmyslnějším kombinacím znaků. Pokud tedy zvolíme jako heslo nějaké slovo (nepoužijeme nesmyslnou kombinaci nejrůznějších znaků), doba prolomení hesla se mnohonásobně zkrátí.

Použité znaky \ Délka hesla		4	5	6	7	8
		Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec
0-9	10 znaků	10 000 2 minuty	100 000 16 minut	1 000 000 3 hodiny	10 000 000 1 den	100 000 000 11 dní
a-z; 0-9	36 znaků	7311616 5 hodin	380204032 7 dní	2×10^9 8 měsíců	8×10^{10} 25 let	3×10^{12} 900 let
a-z; A-Z; 0-9	62 znaků	14776336 2 dny	916132832 3 měsíce	5×10^{10} 18 let	4×10^{12} 1000 let	2×10^{14} 70 000 let
a-z; A-Z; 0-9; ščáéě... ;@#$^*?!...	85 znaků	52200625 6 dní	443705312 1 rok	3×10^{11} 120 let	3×10^{13} 10 000 let	3×10^{15} 800 000 let

Obrázek 1. Doba potřebná k „prolomení“ hesla „hrubou silou“

48.4 Jak tedy na vytvoření hesla?

Nejjednodušší je vymyslet si nějakou větu, kterou si dobře zapamatujeme a podle ní utvořit heslo.

Např.:

- Dvakrát měř, jednou řež. Heslo pak může být 2xm;J5!
- Měla babka 4 jabka a dědoušek jen dvě. Heslo pak může být mb4j+dj2!
- Skákal pes přes oves, přes zelenou louku. Heslo pak může být sPpo,pzl!

Z hlediska bezpečnosti je nejlepší použít např. pro každý server jiné heslo. Bezpečná hesla si lze však jen stěží zapamatovat. Vhodné je využít nějakého programu pro správu hesel (např. volně šiřitelný program KeePass). Takový program má obvykle jedno hlavní centrální heslo (které by mělo být maximálně bezpečné). Po přihlášení do databáze hesel můžete přidávat a generovat neomezeně složitá hesla. Centrální heslo je vhodné také pravidelně měnit.

Otázky, úkoly

- Najdi na Internetu přehled nejpoužívanějších hesel. Pokud mezi nimi najdeš svoje heslo, je to špatně.

Další zdroje ke studiu

- Jak vytvořit silné heslo: http://www.bezpecnyinternet.cz/zacatecnik/hesla/vytvoreni-silneho-hesla.aspx
- Kolik kombinací hesel dokáže dnešní počítač vyzkoušet za minutu?
- Zjsiti, co je to za stroj DES cracker.

Použité zdroje

[1] Přispěvatelé Wikipedie, Bezpečné heslo [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 2. 02. 2012, 20:59 UTC, [citováno 16. 05. 2012] <http://cs.wikipedia.org/w/index.php?title=Bezpe%C4%8Dn%C3%A9_heslo&oldid=7994867>

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-05-16]. Dostupný pod licencí Public domain na WWW: < http://cs.wikipedia.org/wiki/Soubor:Kvalita_hesla.jpg>.

Kryptografie

neboli šifrování je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí.

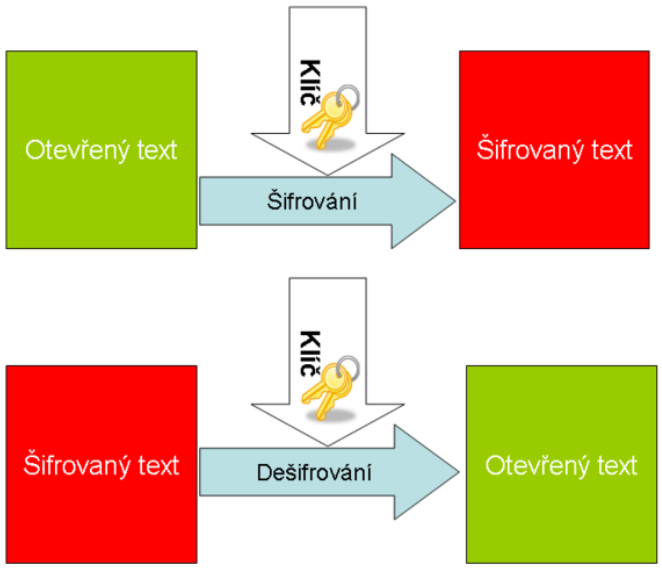
První doložení o zašifrování zprávy pochází z roku 480 př. n. l. za období Řecko-Perských válek v bitvě u Salamíny. Do historie kryptografie se zapsal i významný římský vojevůdce a politik Julius Caesar, a to vynalezením šifry, která byla pojmenována jako Caesarova šifra.

Celé období kryptografie můžeme rozdělit do dvou částí. Tou první je klasická kryptografie, která přibližně trvala do poloviny 20. stol. První část se vyznačovala tím, že k šifrování stačila pouze tužka a papír, případně jiné jednoduché pomůcky. Během 1. poloviny 20. stol. ale začaly vznikat různé sofistikované přístroje, které umožňovaly složitější postup při šifrování. Tím přibližně začala druhá část, kterou nazýváme moderní kryptografie. V dnešní době se k šifrování zpravidla nepoužívají žádné zvlášť vytvářené přístroje, ale klasické počítače.

49. Symetrická kryptografie

Symetrická šifra, někdy též nazývaná konvenční, je takový šifrovací algoritmus, který používá k šifrování i dešifrování jediný klíč. Tím se liší od algoritmů s veřejným klíčem, které mají dvojici klíčů – tajný a veřejný.

Podstatnou výhodou symetrických šifer je jejich nízká výpočetní náročnost. Algoritmy pro šifrování s veřejným klíčem můžou být i stotisíckrát pomalejší. Na druhou stranu velkou nevýhodou je nutnost sdílení tajného klíče, takže se odesilatel a příjemce tajné zprávy musí předem domluvit na tajném klíči.



Obrázek 1. Princip symetrické kryptografie

V praxi existuje celá řada různých symetrických šifer např. AES, DES, RC4, Triple DES, Twofish a celá řada dalších. Vzájemně se liší svojí složitostí, která je často úměrná teoretické době potřebné k jejímu rozluštění. Se stoupající výkonností výpočetní techniky je nutno zdokonalovat „zesložiťovat“ šifry, tak aby bylo možno stále považovat zašifrované informace za bezpečné.

49.1 Historické metody

- **Substituční šifry** - substituční šifra obecně spočívá v nahrazení každého znaku zprávy jiným znakem podle nějakého pravidla.
- **Posun písmen - Caesarova šifra** je pojmenovaná po Juliu Caesarovi, který ji pravděpodobně používal jako první. Každé písmeno tajné zprávy je posunuto v abecedě o pevný počet pozic.
- **Vernamova šifra -** je anglicky často nazývaná one-time pad, v českém překladu jednorázová tabulková šifra. Jde dosud o jedinou známou šifru, o níž bylo exaktně dokázáno, že je nerozluštitelná. Je zde ovšem problém s distribucí klíče.
- **Vigenérova šifra** - jedná se o speciální případ polyalfabetické šifry. Vigenèrova šifra používá heslo, jehož znaky určují posunutí otevřeného textu a to tak, že otevřený text se rozdělí na bloky znaků dlouhé stejně jako heslo a každý znak se sečte s odpovídajícím znakem hesla. Caesarova šifra je tedy speciálním případ Vigenèrovy šifry s heslem o délce jeden znak. Vigenèrova šifra způsobuje změny pravděpodobnosti rozložení znaků a tím podstatně znemožňuje kryptoanalýzu na základě analýzy četnosti znaků v textu. Luštění je založeno na vyhledávání vzdálenosti bigramových či trigramových dvojic v šifrovém textu a určováním jejich společného dělitele vedoucí k zjištění délky hesla.

otevřený text	S	T	A	S	T	N	E	A	V	E	S	E	L	E
klíč	H	E	S	L	O	H	E	S	L	O	H	E	S	L
šifrový text	A	Y	T	E	I	V	J	T	H	T	A	J	E	Q

- **Transpoziční šifry** - transpozice neboli přesmyčka spočívá ve změně pořadí znaků podle určitého pravidla. Například tak, že otevřený text je zapsán do tabulky po řádcích a šifrový text vznikne čtením sloupců téže tabulky.

Otázky, úkoly

- Použil/-la jsi již někde šifrování?
- Existuje bezpečná šifra?
- Proč jsou starší šifry nahrazovány novými?

Další zdroje ke studiu

- Obsáhlý článek o kryptografii/steganografii http://www.security-portal.cz/clanky/praktick%C3%A9-z%C3%A1klady-kryptologie-steganografie

Video

http://www.wimp.com/howencryption/

Použité zdroje

[1] PŘISPĚVATELÉ WIKIPEDIE, Symetrická kryptografie [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 19. 04. 2012, 12:31 UTC, [citováno 24. 07. 2012]<http://cs.wikipedia.org/w/index.php?title=Symetrick%C3%A1_kryptografie&oldid=8431291>

[2] BURDA, Karel, doc. Ing. CSc. *Návrh, správa a bezpečnost počítačových sítí*. FEKT VUT v Brně, Brno 2007.

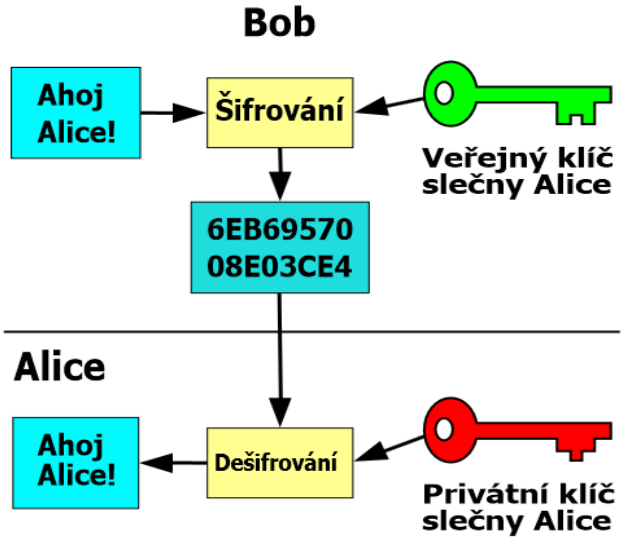
Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-07-24]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Symetrick%C3%A1_%C5%A1ifra.png>.

50. Asymetrická kryptografie

Asymetrická kryptografie (kryptografie s veřejným klíčem) je skupina kryptografických metod, ve kterých se pro šifrování a dešifrování používají odlišné klíče. To je základní rozdíl oproti symetrické kryptografii, která používá k šifrování i dešifrování jediný klíč.

Kromě očividné možnosti pro utajení komunikace se asymetrická kryptografie používá také pro elektronický podpis, tzn. možnost u dat prokázat jejich autora.



Obrázek 1. Princip asymetrické kryptografie.

Základní principy

Šifrovací klíč pro asymetrickou kryptografii sestává z dvou částí: jedna část se používá pro šifrování zpráv (a příjemce zprávy ani tuto část nemusí znát), druhá pro dešifrování (a odesilatel šifrovaných zpráv ji zpravidla nezná). Je vidět, že ten, kdo šifruje, nemusí s dešifrujícím příjemcem zprávy sdílet žádné tajemství, čímž eliminují potřebu výměny klíčů; tato vlastnost je základní výhodou asymetrické kryptografie.

Nejběžnější verzí asymetrické kryptografie je využívání tzv. veřejného a soukromého klíče: šifrovací klíč je veřejný, majitel klíče ho volně uveřejní, a kdokoli jím může šifrovat jemu určené zprávy; dešifrovací klíč je soukromý, majitel jej drží v tajnosti a pomocí něj může tyto zprávy dešifrovat. (Existují i další metody asymetrické kryptografie, ve kterých je třeba i šifrovací klíč udržovat v tajnosti.)

Příklad

Pro pochopení výhod asymetrického šifrování se používá příklad, ve kterém si Alice a Bob posílají zprávy pomocí veřejné pošty. V tomto příkladu Alice posílá utajenou zprávu Bobovi a očekává utajenou odpověď od Boba.

Při použití **symetrické kryptografie** Alice vloží zprávu do schránky a zamkne pomocí visacího zámku, ke kterému má klíč. Schránku poté pošle poštou Bobovi, ten ji otevře použitím kopie Alicina klíče a přečte si zprávu. Bob pak může použít stejný zámek pro odeslání jeho odpovědi.

U **asymetrické kryptografie** má každý svůj visací zámek. Nejdříve Alice požádá Boba, aby jí poslal otevřený zámek bez klíče poštou. Poté jím Alice zamkne zprávu do schránky a tu pošle Bobovi. Bob potom může otevřít zámek svým klíčem a přečíst si zprávu od Alice. K poslání odpovědi musí mít Alicin otevřený zámek, kterým zamkne schránku a pošle ji zpátky Alici.

Největší výhodou tak je, že Alice ani Bob nepotřebují posílat kopii jejich klíče. Tímto se zamezí vytvoření kopie klíče někým třetím během přenosu a odposlouchávání všech následně poslaných zpráv mezi Alicí a Bobem. Nepotřebují tedy věřit poště tolik jako v prvním případě. Navíc, pokud by Bob někomu dovolil si zkopírovat jeho klíč, tak by byly kompromitovány pouze zprávy od Boba, ale všechny zprávy od Alice by zůstaly utajené.

Otázky, úkoly

- Kde všude se dá uplatnit digitální podpis.
- Kde by jsi si zařídil svůj digitální podpis.

Další zdroje ke studiu

- Šifrování pomocí RSA http://www.algoritmy.net/article/4033/RSA

Použité zdroje

[1] PŘISPĚVATELÉ WIKIPEDIE, Asymetrická kryptografie [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 13. 05. 2012, 19:54 UTC, [citováno 24. 07. 2012] <http://cs.wikipedia.org/w/index.php?title=Asymetrick%C3%A1_kryptografie&oldid=8527414>

[2] MIČKA, Pavel. Algoritmus RSA. [online]. [cit. 2012-07-25]. Dostupné z: http://www.algoritmy.net/article/4033/RSA

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-07-24]. Dostupný pod licencí Public domain na WWW: < http://cs.wikipedia.org/wiki/Soubor:Asymetrick%C3%A1_kryptografie.svg>.

51. Nové využití kryptografie

Počítačová revoluce přinesla řadu nových myšlenek do oblasti využití kryptografie:

51.1 Jednosměrné funkce

První z nich jsou jednosměrné funkce. Jsou to takové funkce f: X → Y, pro něž je snadné z jakékoli hodnoty x ∈ X vypočítat y = f(x), ale pro nějaký náhodně vybraný obraz y ∈ f(X) nelze (neumíme, je to pro nás výpočetně nemožné) najít její vzor x ∈ X tak, aby y = f(x). Přitom víme, že takový vzor existuje nebo jich existuje dokonce velmi mnoho. Je to třeba, jako když smícháme dvě složky lepidla. Za několik vteřin vytvoří novou sloučeninu se zcela novými vazbami atomů a molekul, které nelze jednoduše rozpojit a vrátit do původní podoby.

Podobně to probíhá s ohromnými čísly. Dokážeme je snadno spojit vynásobením. Číslo, které obdržíme, má však zcela jinou "molekulární" strukturu, původní dvě složky pevně váže v nové číselné sloučenině a my v současné době neznáme dostatečně rychlou metodu jak tato čísla separovat.

51.2 Hašovací funkce

První odnoží jednosměrných funkcí jsou tzv. hašovací funkce, které umí vytvořit z jakkoliv velkých dat jejich identifikátor - digitální otisk dat. Data lze nyní identifikovat (a to i z právního hlediska) podle jejich digitálního otisku majícího řádově pár set bitů.

Kontrola shody databází, otisky dat

Uveďme si příklad banky, která ukládá všechna data ze všech účtů klientů do databázového systému, který je on-line zálohován, takže se vyskytuje současně na třech, geograficky vzdálených místech Evropy. V určitý okamžik je nutné zjistit, zda tyto systémy jsou opravdu totožné. Proto na určitou dobu uvedeme databáze do klidu. Nyní bychom mohli klasicky přenášet z jednoho i druhého záložního centra jednotlivé sektory pevných disků nebo záznamy v databázi do centra a porovnávat je řetězec za řetězcem. Možná za několik dní nebo týdnů bychom mohli být hotovi, v závislosti na objemu dat a přenosové kapacitě spojení.

Místo toho však stačí na všech třech místech vypočítat pouze hašový obraz databází nebo jednotlivých jejich částí (sekcí apod.) f(db) a přenést tyto obrazy k porovnání do centra. Na rozdíl od jejich vzorů se jedná jen o stovky bitů. Pokud jsou hodnoty $f(db_1)$, $f(db_2)$ a $f(db_3)$ shodné, máme jistotu, že se databáze nebo jejich části neliší ani o jeden bit. Digitální otisky dat působí stejně jako otisky

prstů. V řadě zemí byly digitální otisky dat z hlediska identifikace dat nepřímo legislativně postaveny na roveň otisků prstů.

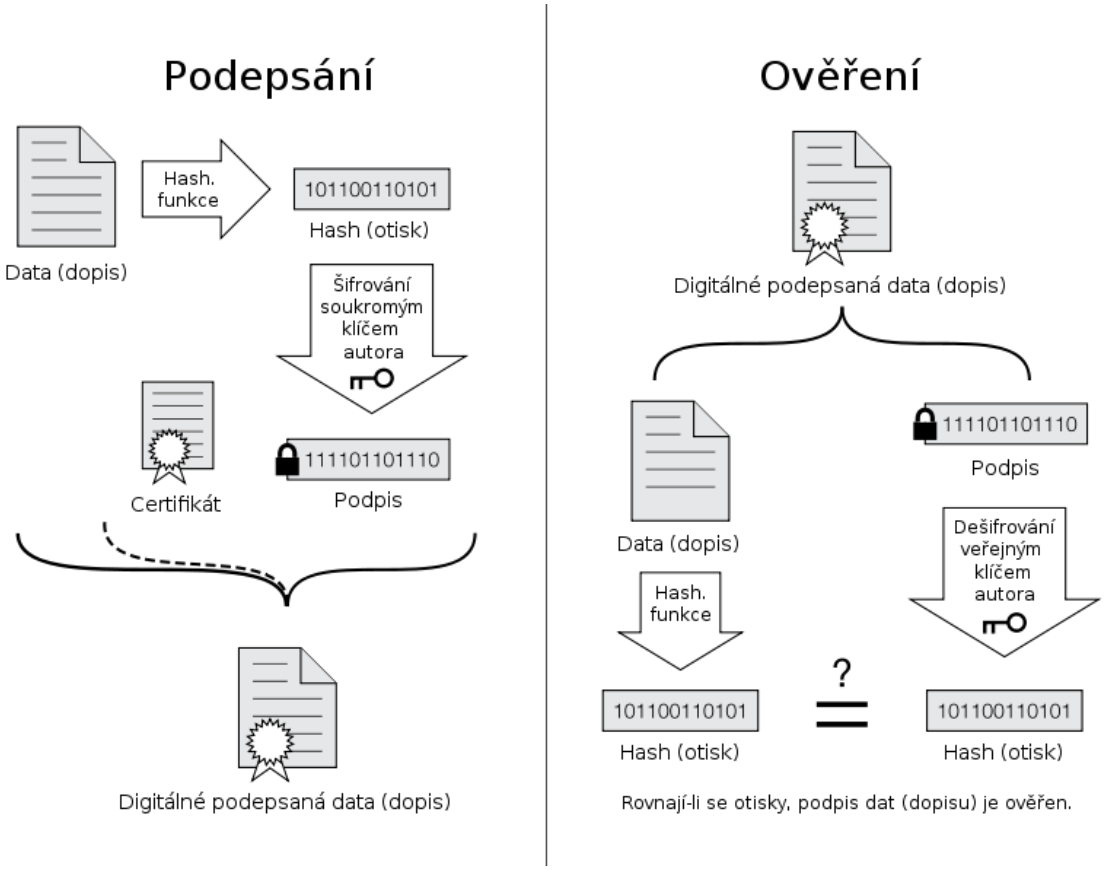
51.3 Ukládání přihlašovacích hesel

Další zajímavou aplikací hašovacích funkcí je ukládání přihlašovacích hesel v počítačových systémech. Hesla uživatelů, nemohou být ukládána do systémů přímo, protože by je šlo jednoduše vyhledat a zneužít. Ukládají se proto ve formě $h(pswd_i)$, kde h je hašovací funkce. Díky její jednocestnosti není z této hodnoty, uložené v systému, možné odvodit vlastní hodnotu přihlašovacího hesla pswdi, vyloučíme-li snadné passwordy a slovníkový útok na ně. V reálných systémech se navíc používá metoda solení znesnadňující slovníkový útok.

51.4 Digitální podpis

Druhým případem užití asymetrické kryptografie je digitální podpis. Představme si, že chceme vydat důležité prohlášení, ale nepřejeme si, aby s ním kdokoliv manipuloval, a zároveň chceme, aby si každý mohl ověřit, že jsme jej skutečně napsali my (tzn., že se za nás nikdo nevydává).

V případě asymetrické kryptografie pouze zhotovíme *hash* (otisk zprávy), zašifrujeme jej svým soukromým klíčem a výsledný řetězec přiložíme ke zprávě. Tuto dvojici poté odešleme (samotná zpráva není nijak šifrována, aby si ji mohl kdokoliv přečíst). Každý, kdo si bude chtít ověřit, že je zpráva autentická, může dešifrovat otisk pomocí našeho veřejného klíče a porovnat jej s vlastnoručně vytvořeným otiskem příchozí zprávy. Pokud jsou otisky totožné, tak příjemce ví, že jsme zprávu napsali my, a že s ní nebylo nijak manipulováno.



Obrázek 2. Diagram ilustruje podepsání a ověření dat (dopisu) elektronickým podpisem

Otázky, úkoly

- Kde všude se dá uplatnit digitální podpis.
- Kde by jsi si zařídil svůj digitální podpis.

Další zdroje ke studiu

- Šifrování pomocí RSA http://www.algoritmy.net/article/4033/RSA

Použité zdroje

[1] MIČKA, Pavel. Algoritmus RSA. [online]. [cit. 2012-07-25]. Dostupné z: http://www.algoritmy.net/article/4033/RSA

[2] KLÍMA, Vlastimil. Základy moderní kryptologie – Symetrická [online]. 5.4.2005. [cit. 2012-07-25]. Dostupné z: http://crypto-world.info/klima/mffuk/Symetricka_kryptografie_I_2006.pdf

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-07-24]. Dostupný pod licencí Public domain na WWW: <http://cs.wikipedia.org/wiki/Soubor:Digital_Signature_diagram_cs.svg>.

52. Nebezpečí pro sítě – bezpečnost spojů

Možnosti útočníka

- vyřazení spoje (přerušení kabelu nebo rušení kmitočtu),
- odposlech přenášených informací,
- modifikace přenášených informací.

52.1 Ochrana před vyřazením spoje

- redundance sítě: používat síťové struktury, ve kterých existuje více nezávislých cest,
- fyzická ochrana kabelových spojů: ztížit útočníkovi fyzický přístup ke spoji (např. umístěním spoje v kontrolované zóně, přepojovačů v uzavřené místnosti apod.),
- technická ochrana rádiových spojů: ztížit útočníkovi možnost rušení spoje (např. techniky rozprostření spektra nebo adaptace kmitočtu).

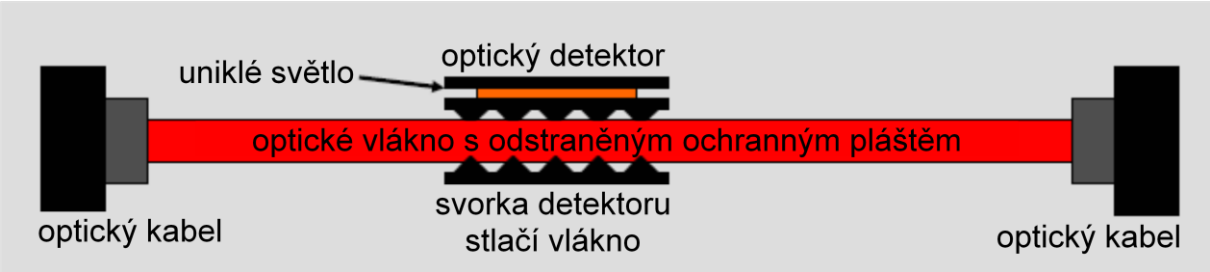
52.2 Odposlech přenášených informací:

- odposlechem spojů může útočník získat velmi cenné informace,
- nejsnadněji lze odposlouchávat rádiové spoje, ale není problém odposlouchávat metalické i optické kabely.

Odposlech optického kabelu

Zařízení "clip-on coupler" (rozměry 6x8x8 cm, cena 30 tis. Kč),

Založeno na tom, že při ohybu ("bend") vlákna se změní úhel dopadu některých paprsků. Dojde tak k překročení mezního úhlu odrazu a daný paprsek opustí vlákno. Tento únik lze detekovat a sledovat tak přenášené informace.



Obrázek 1. Odposlech optického kabelu.

Přenos dat pomocí kvantové kryptografie

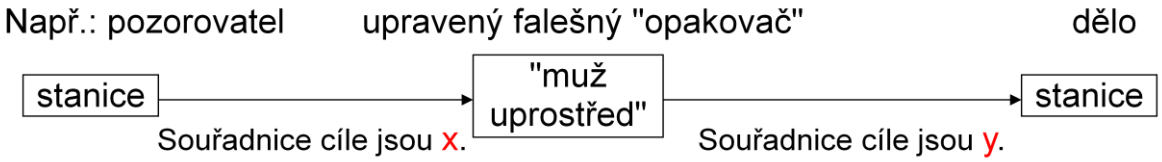
Kvantová kryptografie je využitím kvantové mechaniky k bezpečné distribuci klíčů a umožňuje spolehlivě detekovat případný odposlech. V principu by měla

být neprolomitelná, v praktické realizaci však existují slabiny, které mohou být zneužity k prolomení bezpečnosti.

Kvantová kryptografie je s největší pravděpodobností budoucností šifrování.

52.3 Modifikace přenášených informací

Útočník modifikací přenášených informací může způsobit značné ztráty.



Obrázek 2. Modifikace přenášených dat metodou „muž uprostřed“.

Otázky, úkoly

- Chráníš nějak svoji domácí síť proti zneužití?
- Jakým způsobem se nejčastěji přijde na zneužití sítě?

Další zdroje ke studiu

- Informace o kvantové kryptografii http://cs.wikipedia.org/wiki/Kvantov%C3%A1_kryptografie
- Článek na lupě o kvantové kryptografii http://www.lupa.cz/clanky/kvantova-kryptografie-pro-bezpecnou-distribuci-klicu/

Použité zdroje

[1] BURDA, Karel, doc. Ing. CSc. *Návrh, správa a bezpečnost počítačových sítí*. FEKT VUT v Brně, Brno 2007.

Použité obrázky

[1]

53. Útoky na data v sítí

53.1 Útoky v linkové vrstvě 802.3

1) útok přetečením paměti přepínače (MAC flooding)

- přepínač si vede přepínací tabulku (MAC adresa - číslo portu),
- útočník z jednoho portu vysílá sérii rámců s různými MAC adresami. Přepínač proto musí rozšiřovat přepínací tabulku až do doby, kdy vyčerpá přidělenou paměťovou kapacitu. Od toho okamžiku začne pracovat jako hub, tj. veškeré rámce vysílá do všech portů.
- útočník tak do svého portu soustředí veškeré rámce zpracovávané daným přepínačem,
- ochrana
  - některé přepínače dovolují na svých portech přednastavit povolené MAC adresy,
  - některé přepínače dovolují odstavit port, ze kterého přicházejí rámce s více MAC adresami.

2) útok zneužitím ARP protokolu (ARP spoofing)

- stanice LAN si vedou tabulky (MAC adresa - IP adresa),
- aktualizace tabulky se provádí ARP protokolem. Pomocí ARP protokolu se stanice může dozvědět MAC adresu nějakého zařízení o známé IP adrese. V síti rozešle dotaz a příslušná stanice ji zašle odpověď. Odpověď obsahuje přiřazení (MAC adresa - IP adresa) jak tazatele tak i odpovídajícího,
- útočník z jednoho portu vysílá tyto odpovědi, kde pro cílovou IP adresu (IPx) uvádí svoji MAC adresu. Přepínač zašle tyto rámce vybraným počítačům, které pak budou pakety pro adresáta IPx zasílat na stanici útočníka. Útočník tyto pakety monitoruje a dále přeposílá skutečnému adresátovi.
- je útok, kdy útočník ve vysílaných uvádí neexistující MAC adresu. Tím dojde ke znemožnění komunikace, protože zaslané pakety nemá kdo předávat správnému adresátovi.
- ochrana: statické ARP záznamy ve stanicích.

53.2 Útoky v transportní vrstvě

Záplavový útok pomocí TCP protokolu

Nejznámější záplavový útok (tzv. "SYN flood") využívá zprávu "SYN".

Útočník odešle oběti zprávu SYN. Zdrojová adresa i port jsou smyšlené.

Oběť si pro toto nové TCP spojení vyčlení vyrovnávací paměti a neexistujícímu protějšku zašle zprávu "SYN+ACK". Na tu mu nikdo neodpoví. Po

nastavené době zkusí tuto zprávu zopakovat. V případě neúspěchu vyčleněné kapacity uvolní.

Pokud je však intenzita zpráv "SYN" vysoká, může dojít k tomu, že se řádní uživatelé nemohou připojit, protože je připojovací kapacita oběti vyčerpána.

K ochraně se používá metoda "SYN cookies".

Server nevyčlení žádné paměťové kapacity a zprávu "SYN+ACK" (tzv. "SYN cookies") odešle.

Pokud nedojde odpověď ACK, tak se nic neděje - žádné prostředky serveru nebyly tímto "spojením" vázány.

53.3 Vyřazení serveru

V tomto typu útoku se využívá skutečnosti, že zpracováním přijatých dat může dojít k nestandardní situaci, která může vést k pádu nebo zatuhnutí operačního systému.

Známý je útok založený na chybně naprogramované defragmentaci paketu (tzv. "Teardrop attack").

Oběti jsou zaslány dva fragmenty, přičemž jeden fragment se částečně nebo zcela překrývá s druhým fragmentem. Operační systém při pokusu složit z těchto fragmentů původní paket zatuhne.

53.4 Útoky na odepření služby

Útok na odepření služby ("Denial of Service" - DoS): cílem útoku je znemožnit poskytování nějaké služby (např. prohlížení www stránek, surfování) uživatelům této služby.

Metody:

- zahlcení linky (tzv. záplavový útok): do linky uživatele nebo serveru jsou směrována neužitečná data znemožňující přenos dat žádaných.

Tento typ útoku existuje v mnoha variantách a obrana vůči němu je poměrně omezená.

- vyřazení serveru: vyšlou se taková data, že při jejich zpracování dojde k nestandardní situaci, která vede pádu nebo k zatuhnutí operačního systému počítače (např. přetečení zásobníku).

Otázky, úkoly

- Proč se dnes častěji vedou útoky na vyřazení serveru než útoky vedoucí ke získání dat ze serveru?

Další zdroje ke studiu

- Článek na Lupě o funkci útoků DoS http://www.zive.cz/clanky/jak-funguje-ddos-hlavni-zbran-kybervalky/sc-3-a-155080/default.aspx

Použité zdroje

[1] BURDA, Karel, doc. Ing. CSc. *Návrh, správa a bezpečnost počítačových sítí*. FEKT VUT v Brně, Brno 2007.

54. Steganografie

Steganografie (řečtina. steganós-schovaný, gráphein-psát) je vědní disciplína (podobor kryptografie) zabývající se utajením komunikace prostřednictvím ukrytí zprávy. Zpráva je ukryta tak, aby si pozorovatel neuvědomil, že komunikace vůbec probíhá. Sem patří různé neviditelné inkousty, vyrývání zprávy do dřevěné tabulky, která se zalije voskem apod. V moderní době lze tajné texty ukrývat například do souborů s hudbou či obrázky namísto náhodného šumu. Síla této komunikace stojí a padá na jejím utajení (jedná se o takzvanou bezpečnost skrze utajení – security through obscurity) a proto zachycení skryté zprávy tak prakticky znamená její prolomení. Aby ani v tom případě nedošlo k prozrazení obsahu zprávy, zpravidla se kombinuje s dalšími metodami šifrování.

Příklad steganografie: V tomto obrázku:

je vložen tento obrázek:

V informačním věku se steganografie stále uplatňuje, ale změnila podobu v souvislosti s rozmachem informačních technologií. Tajná zpráva může být zakódována na místo nepodstatného šumu v souborech se zvuky, obrázky, videem a podobně. Častou aplikací steganografie při kódování informací do obrázků může být i chránění děl podle autorského práva.

Některé počítačové tiskárny jsou schopny zaznamenat (do kódu tvořeného tečkami žlutým inkoustem, tisknutým na okraje nebo zadní stranu papíru) své sériové číslo a datum a čas tisku.

Konvenční metodou konkrétně u obrázku s 24bitovým barevným prostorem RGB (8 bitů na jednu ze tří základních barevných složek) je odstranit z každého barevného kanálu každého pixelu zdrojového obrázku dva nejméně podstatné bity a ty použít do obrázku vloženého. Cílový obrázek bude nižší kvality, ale lidské oko ztrátu informace z původního obrázku nebude prakticky schopno zaregistrovat.

Nejvhodnější jsou nekomprimované soubory, a to zejména kvůli jejich velikosti, kdy do nich lze umístit větší objem dat anebo je lépe uschovat. Ideální jsou obrázky obsahující mnoho detailů. Na bílém pozadí se bude informace velmi těžko schovávat. Skrývaný soubor nesmí mít větší velikost, než původní nosné médium. Problém nastává při případné kompresi či změně formátu, kdy dochází vlivem kompresního algoritmu k poškození a zničení zprávy.

Moderní Steganografie

Mezi další zajímavý typ co se týče už moderní steganografie je její kombinace s kódy (kódy blíže dále), kdy díky veřejným sdělovacím prostředkům (rádio, rozhlas), denního tisku (inzeráty, či cenzurované korespondence obě strany můžou komunikovat díky zprávám opravdu nevinného významu.

Jelikož v dnešní době už žijeme ve věku počítačů, ve kterých se nachází opravdu spousta datových formátů, do kterých je velmi snadné zprávu ukrýt, to nabízí tzv. digitální steganografie. Zprávu můžeme přibalit i do textových, či datových souborů ale nejlépe můžeme informace schovat v grafických (bitmap), nebo zvukových formátech, kterou jsem nosiči určitého „šumu“ aniž by byly znehodnoceny.

Využití steganografie má i své stinné stránky. Na veřejnost pronikla zpráva, že steganografii využívali teroristé, přičemž tajné zprávy ukrývali do obrázků na webech, jako jsou Amazon, nebo eBay. Následný rozsáhlý průzkum téměř dvou milionů obrázků z eBay nenašel, ani neprokázal jedinou tajnou zprávu. Avšak automaticky byla steganografie označena za terorismus a takového označení se velmi špatně zbavuje.

Možnosti aplikace steganografie

Oblasti kde můžeme steganografii aplikovat jsou z podstaty věci často nezákonné. Nelze steganografii jako takovou odsoudit za nástroj teroristům, jelikož celá oblast skrývání informací může být naopak velmi užitečná.

Otázky, úkoly

- Vyhledej na internetu nějaký obrázek, který má stefanograficky ukrytou informaci.

Další zdroje ke studiu

- Steganografie v praxi http://www.root.cz/clanky/jak-ukryt-tajna-data-do-obrazku-aneb-steganografie-v-praxi/

Použité zdroje

[1] Přispěvatelé Wikipedie, Kryptografie [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 13. 05. 2012, 21:44 UTC, [citováno 24. 05. 2012] <http://cs.wikipedia.org/w/index.php?title=Kryptografie&oldid=8528114>

[2] Přispěvatelé Wikipedie, Steganografie [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 9. 04. 2012, 20:05 UTC, [citováno 24. 05. 2012] <http://cs.wikipedia.org/w/index.php?title=Steganografie&oldid=8370708>

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-08-24]. Dostupný pod licencí Public domain na WWW: < http://cs.wikipedia.org/wiki/Soubor:StenographyOriginal.png>.

[2] Commons.wikimedia.org [online]. [cit. 2012-08-24]. Dostupný pod licencí Public domain na WWW: < http://cs.wikipedia.org/wiki/Soubor:StenographyRecovered.png>.

55. Návrh a realizace jednoduché sítě

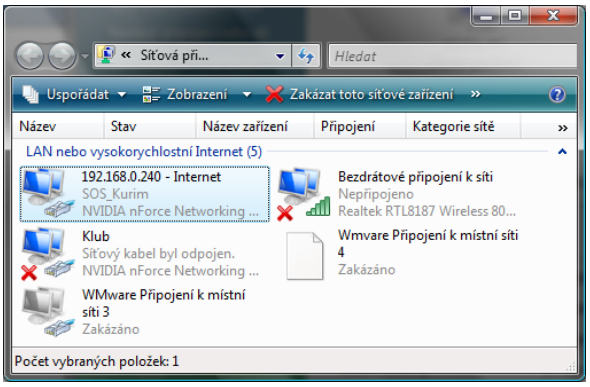
55.1 Přímé propojení dvou počítačů kabelem

Co potřebujeme?

Křížený síťový UTP kabel s konektory RJ-45, kterým propojíme síťové karty obou počítačů.

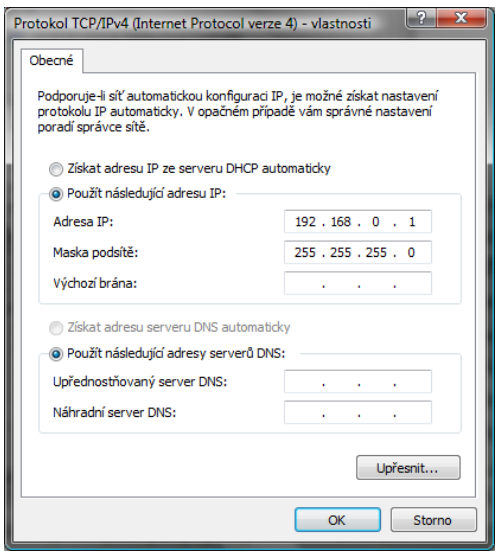
Co nastavíme?

Vyberte v nabídce „Start“ > „Ovládací panely“ > „Síťová připojení“ správné připojení.



Obrázek 1. Výběr síťového připojení ke konfiguraci

Z kontextové nabídky vyberte Vlastnosti a přejděte na záložku „Obecné“. Vyberte „Protokol sítě internet (TCP/IP)“ a klikněte na „Vlastnosti“. V otevřeném okně je nutné správně nakonfigurovat IP adresy, zvolte „Použít následující adresu IP“ a do pole „Adresa IP“ vložte 192.168.0.1, do pole „maska podsítě“ 255.255.255.0.



Obrázek 2. Ruční nastavení IP adresy.

Druhý počítač nastavte stejně, ale místo IP adresy 192.168.0.1 použijte jinou, nejlépe 192.168.0.2 (v síti nesmí být dva počítače se stejnou IP adresou). Navíc pro pozdější použití sdíleného internetu můžete nastavit další následující údaje (pro sdílení dat a hraní síťových počítačových her to však není nutné), do pole „výchozí brána“ vložte 192.168.0.1, dále zvolte „použít následující adresy serverů DNS“ a do prvního pole vložte taktéž 192.168.0.1, stiskněte „OK“ a nastavení se aktivuje. Nyní propojte počítače síťovým kabelem a počítače mezi sebou aktivují spojení.

55.2 Připojení počítačů k internetu pomocí routeru

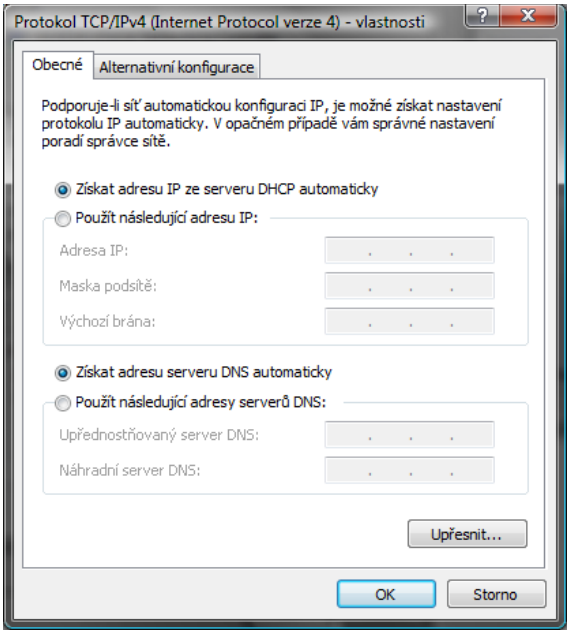
Co potřebujeme?

Router, přímé síťové UTP kabely s konektory RJ45.

Co nastavíme?

Je-li na routeru zapnut DHCP server pro místní síť, nakonfigurujeme počítače tak aby získaly IP adresu automaticky. V nastavení síťového připojení, ve vlastnostech „Protokol sítě internet (TCP/IP)“ zatrhneme volbu „získat adresu IP ze serveru DHCP automaticky“, taktéž u nastavení DNS zvolte „získat adresu serveru DNS automaticky“. (

Pokud by router neměl zapnut DHCP server, tak je potřeba nastavit pro prvotní spojení a konfiguraci statickou IP adresu, to už umíme díky prvnímu návodu – jak propojit dva počítače (jakou IP adresu nastavit, najdete v manuálu).



Obrázek 3. Nastavení získání IP adresy z DHCP serveru.

Nyní se můžete připojit na router (router se zpravidla konfiguruje přes webové rozhraní – adresa, přes kterou se na něj připojíte, bývá většinou výchozí

brána, viz manuál k routeru) a nakonfigurovat WAN port, do kterého se zapojuje venkovní síť (internet) – údaje, dle kterých ho nakonfigurovat, si vyžádejte od internetového poskytovatele nebo správce sítě. Nyní propojte ostatní počítače s routerem (pro připojení většího množství počítačů lze použít k routeru ještě switch).

Obrázek 4. Webové rozhranní pro konfiguraci AP/routeru

Otázky, úkoly

Vyzkoušej si uvedené postupy

Použité zdroje

[1] JE, David. *Základy PC: počítačové sítě snadno a rychle*, [online]. Publikováno 18. 9. 2006 [citováno 24. 08. 2012]. <http://pctuning.tyden.cz/navody/zaklady-stavba-pc/7543-zaklady_pc-pocitacove_site_snadno_a_rychle>.

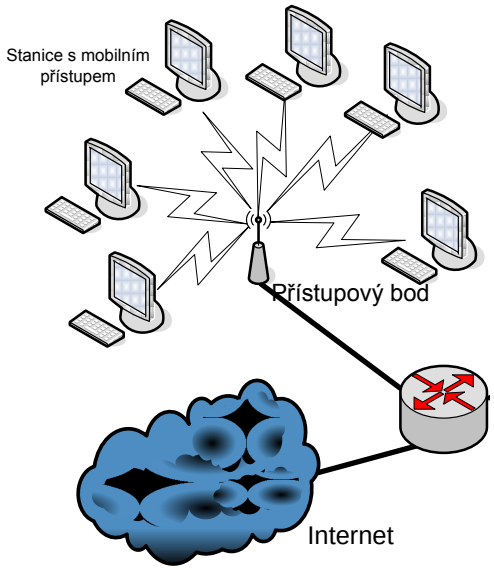
Použité obrázky

[1] Autorem obrázků je Vojtěch Novotný.

56. Připojení pomocí WiFi Access pointu

Co potřebujeme?

WiFi Access point (AP), přímé síťové kabely s konektory RJ45 (pro počáteční konfiguraci), počítač s WiFi.



Obrázek 1. Síť s bezdrátovým přístupem k pevné síti

Co nastavíme?

Nejdříve je potřeba na AP nastavit a zabezpečit bezdrátovou sítě. Následně nastavit zabezpečení i u klientů (na počítačích) a až pak se do bezdrátové sítě připojit.

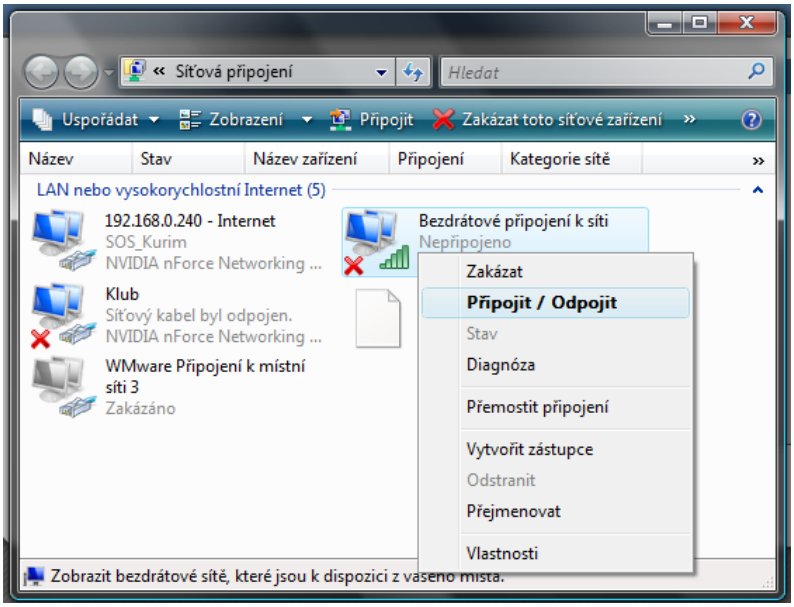
K AP tedy připojíme počítač nejdříve kabelem kvůli nakonfigurování bezdrátové sítě. To provedeme dle předchozího návodu (jakou IP adresu nastavit, najdete v manuálu). Zjednodušené nastavení bezdrátové sítě v AP:

- Zadejte jméno sítě „SSID“ (libovolný identifikátor vaší sítě).
- Vyberte kanál, na kterém bude pracovat – „Channel“ (bývá 1 až 13). Vyberte nejlépe kanál, který ve vašem okolí nikdo nevyužívá (volné kanály zjistíte v lepších AP nebo např. pomocí programu netstumbler).
- Dále vyberte typ zabezpečení (zabezpečení je velice důležité, bez něho by byla vaše síť „otevřená“ a přístupná komukoli, kdo bude v jejím dosahu). Jediné vcelku bezpečné zabezpečené je WPA2 s přístupovým klíčem, který může mít 8 – 63 znaků (doporučuji použít velká i malá písmena, čísla i speciální znaky a nezapomeňte si klíč poznamenat). Zabezpečení bezdrátové sítě lze mírně zvýšit přidáním MAC filtru a vypnutím DHCP serveru (tedy s použitím statických adres).
- Nakonec zkontrolujte, jestli máte zapnut DHCP server.

- Nastavení uložte, AP následně restartujte.

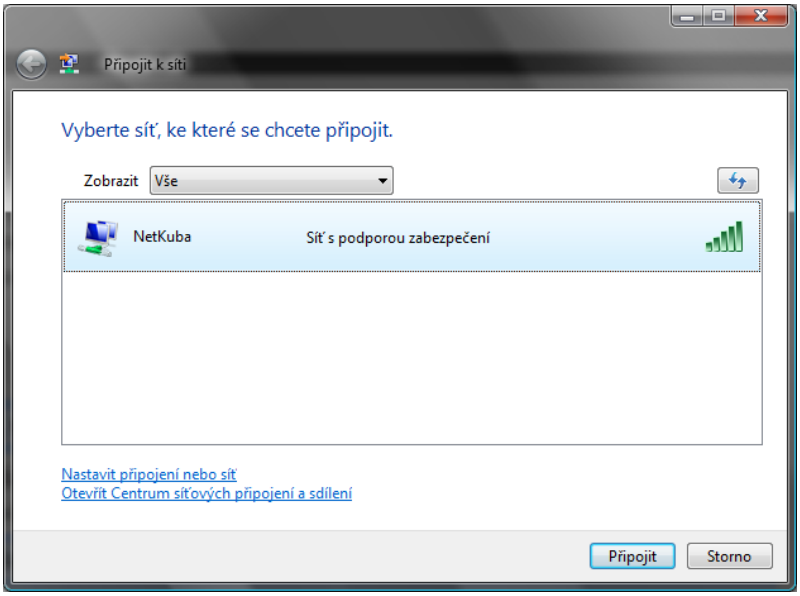
Odpojte kabelem připojený počítač od AP. Nyní máme připravenou bezdrátovou síť a můžeme do ní připojit počítače.

V počítači vyberte v nabídce „Start“ > „Ovládací panely“ > „Síťová připojení“ správné bezdrátové připojení. Z kontextové nabídky vyberte Připojit/Odpojit.



Obrázek 2. Připojení k bezdrátové síti

V otevřeném okně kliknete na „aktualizovat seznam sítí“, seznam se aktualizuje a zobrazí dostupné bezdrátové sítě, zvolte tu vaší a připojte se k ní, během připojování budete požádáni o vložení přístupového klíče, který jste zvolili pro zabezpečení sítě. Po zadání správného klíče dostane počítač od přístupového bodu přiřazenou IP adresu a je připojen do sítě.



Obrázek 3. Výběr bezdrátové sítě

Otázky, úkoly

Vyzkoušej si uvedené postupy

Použité zdroje

[1] JE, David. *Základy PC: počítačové sítě snadno a rychle*, [online]. Publikováno 18. 9. 2006 [citováno 24. 08. 2012]. <http://pctuning.tyden.cz/navody/zaklady-stavba-pc/7543-zaklady_pc-pocitacove_site_snadno_a_rychle>.

Použité obrázky

[1] Autorem obrázků je Vojtěch Novotný.

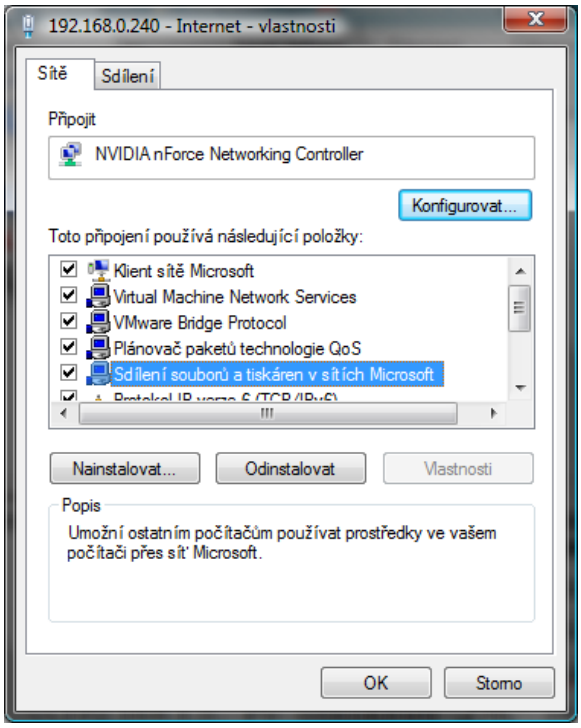
57. Sdílení souborů a tiskáren v lokální síti

57.1 Sdílení souborů

Nejprve je třeba zkontrolovat, jestli je sdílení souborů a tiskáren ve Windows nainstalované. Postupujte následovně: Otevřete si „vlastnosti“ vašeho síťového připojení („Start“ > „Ovládací panely“ > „Síťová připojení“) a v tabulce vidíte položky, jaké vaše síťové připojení využívá, pokud tam není vypsané „sdílení souborů a tiskáren v sítích Microsoft“, pak je třeba podporu sdílení doinstalovat.

Klikněte na tlačítko „Nainstalovat…“ v novém okně vyberte „služba“ a dejte „přidat“. Vyberte „sdílení souborů a tiskáren v sítích Microsoft“, pokračujte tlačítkem „OK“. Služba se nainstaluje a přidá se k vašemu síťovému připojení, můžete pokračovat stisknutím tlačítka „zavřít“.

Nyní je vše připraveno k nasdílení dat do sítě.

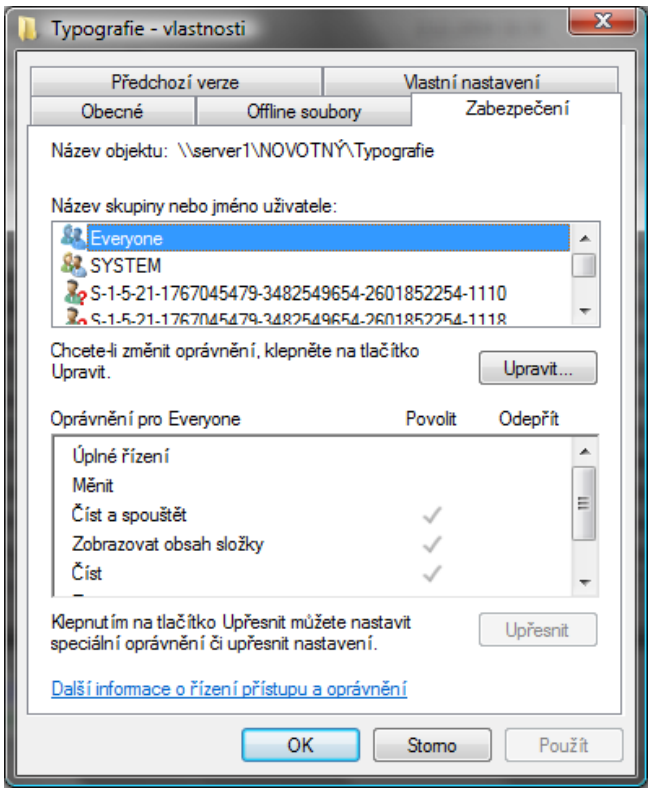


Obrázek 1. Nainstalovaná služba sdílení souborů a tiskáren v sítích Microsoft

Klikněte na adresář, který chcete sdílet pravým tlačítkem a vyberte „sdílení a zabezpečení“. Zaškrtněte políčko „složka sdílená v síti“, zaškrtnutím políčka „povolit uživatelům v síti měnit mé soubory“ povolíte, jak je již patrné, uživatelům mazat a měnit vaše soubory, pokud si tím nejste opravdu jisti, políčko nechte raději nezaškrtnuté. Nyní je vybraný adresář k dispozici ostatním uživatelům v síti. Když na jiném počítači tedy otevřete „místa v síti“, uvidíte nasdílená data z počítače, na kterém jsme sdílení nastavovali. Někdy se stane, že místo nasdílených dat nevidíte zhola nic, lze si pomoci následujícím postupem – klikněte na „Start“ > „Spustit“ a do pole napište dvě zpětná lomítka a název

počítače, na kterém jsou nasdílená data (nebo jeho IP adresu) \\Server1 nebo \\192.168.0.252. Po odkliknutí „OK“ se otevře volaný počítač a lehce se již dostanete ke sdíleným datům.

Po nasdílení je složka dostupná komukoli v síti. To může být pro někoho nežádoucí a tak je možnost ji zpřístupnit jen vybraným uživatelům pomocí "složitého sdílení". K jeho nastavení se dostanete například přes Průzkumníka, v něm otevřete v menu "Nástroje" > "Možnosti složky" > "Zobrazení" a v okně odškrtněte "použít zjednodušené sdílení souborů". Nyní při povolování sdílení složky máte mnohem větší možnosti nastavení (přiřadit práva jednotlivým uživatelům).

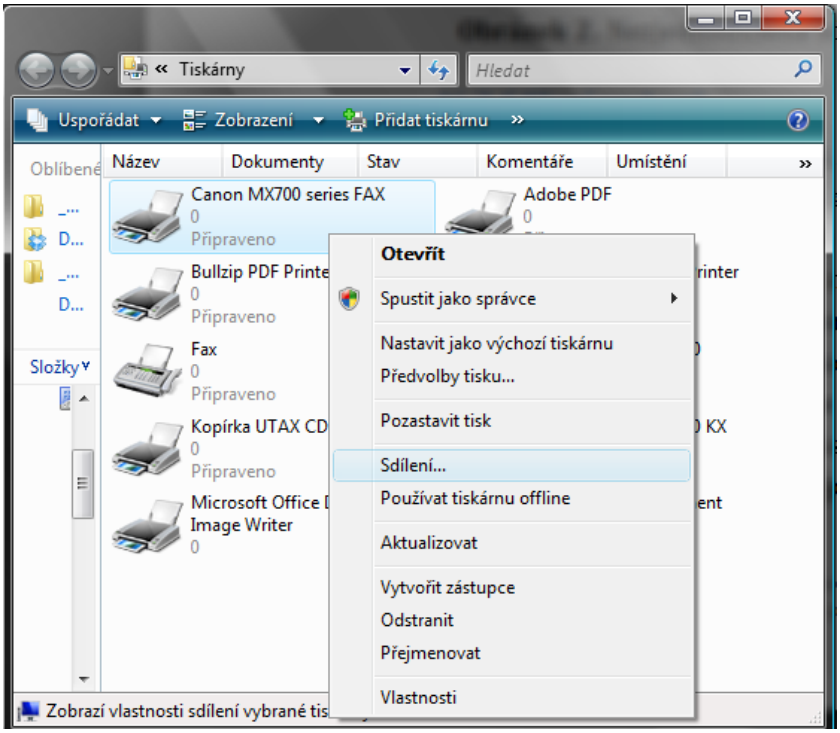


Obrázek 2. Nezjednodušené sdílení souborů a složek – nastavení práv.

57.2 Sdílení souborů

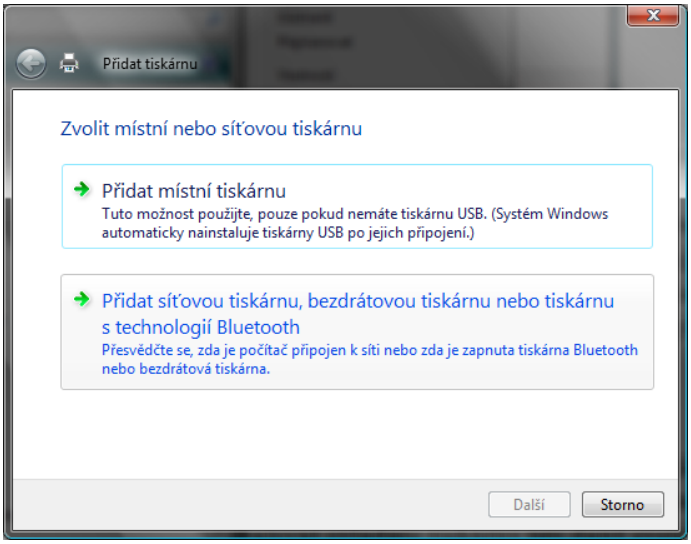
Pokud jsme nepořídili tiskárnu, která je vybavena síťovou kartou je nutné tiskárnu připojit k jednomu počítači a pro ostatní je nasdílet.

Tiskárna se musí nasdílet podobně jako data. Otevřete si („Start“ > „Ovládací panely“ > „Tiskárny“), na tiskárnu, kterou chcete sdílet ostatním počítačům, klikněte pravým tlačítkem a zvolte „sdílení“.



V nově otevřeném okně, v záložce „sdílení“, zvolte „sdílet tuto tiskárnu“ a můžete napsat její jméno, které se v síti bude zobrazovat. Potvrďte „OK“.

Na ostatních počítačích je třeba jen tiskárnu připojit, provedete to následovně. Otevřete si („Start“ > „Ovládací panely“ > „Tiskárny“), vyberte volbu Přidat tiskárnu. Vyberte Přidat síťovou tiskárnu… a pomocí průvodce se tiskárna přidá. Většinou (při rozdílných OS) je potřeba do počítače s tiskárnou doinstalovat ovladače tiskárny.



Obrázek 3. Instalace nasdílené tiskárny.

Nesmíte ale zapomenout, že tisk ze sítě je možný, jen když bude počítač, na kterém je tiskárna zapojena, zapnutý!

Otázky, úkoly

- Vyzkoušej si uvedené postupy

Použité zdroje

[1] JE, David. *Základy PC: počítačové sítě snadno a rychle*, [online]. Publikováno 18. 9. 2006 [citováno 24. 08. 2012]. <http://pctuning.tyden.cz/navody/zaklady-stavba-pc/7543-zaklady_pc-pocitacove_site_snadno_a_rychle>.

Použité obrázky

[1] Autorem obrázků je Vojtěch Novotný.

58. Softwarová podpora diagnostiky sítě

Operační systém Windows v příkazovém řádku obsahuje některé diagnostické nástroje protokolu TCP/IP. Operační systém Linux je zpravidla vybaven pro diagnostiku mnohem lépe.

Přehled příkazů pro OS z rodiny Windows.

ARP

Umožňuje zobrazit a upravit obsah mezipaměti protokolu ARP (Address Resolution Protocol). Tato mezipaměť obsahuje místní tabulku používanou k převádění adres IP na adresy řízení přístupu k médiím používané v místní síti.

Hostname

Vrací hostitelský název místního počítače.

Ipconfig

Zobrazí aktuální konfiguraci protokolu TCP/IP. Používá se také k ručnímu uvolnění a obnovení konfigurací TCP/IP přiřazených serverem DHCP.

LPQ

Načítá informace o stavu tiskové fronty z počítačů vybavených tiskovým serverem LPD (Line Printer Daemon).

Nbtstat

Zobrazí místní tabulku názvů NetBIOS (tabulka názvů NetBIOS registrovaných místními programy) a mezipaměť názvů NetBIOS (výpis místní mezipaměti názvů počítačů používaných v protokolu NetBIOS, které byly převedeny na adresy IP).

Netsh

Používá se k zobrazení a správě nastavení protokolu TCP/IP v místním nebo vzdáleném počítači.

Netstat

Zobrazí informace o relaci protokolu TCP/IP.

Nslookup

Kontroluje záznamy, aliasy hostitelů v doméně, služby hostitelů v doméně a informace o operačním systému prostřednictvím dotazů na servery DNS.

Ping

Ověří konfiguraci a zkontroluje funkčnost připojení IP.

Route

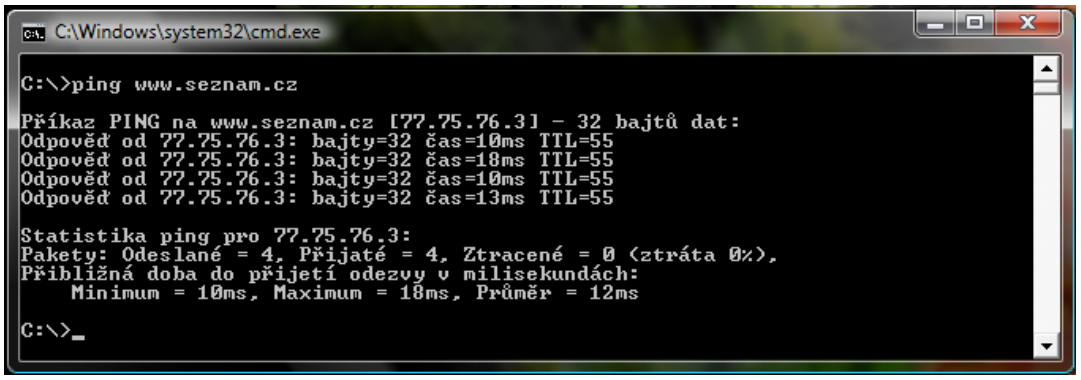
Zobrazí nebo upraví obsah místní směrovací tabulky.

Tracert

Zobrazí trasu, po které jsou pakety přenášeny na zadanou cílovou adresu (Trasování cesty pomocí příkazu tracert).

Pathping

Zobrazí trasu, po které jsou přenášeny pakety na zadanou cílovou adresu, spolu s informacemi o ztrátách paketů pro jednotlivé směrovače na této trase. Příkaz Pathping lze také využít k řešení potíží s funkcí připojení QoS (Quality of Service).



Obrázek 1. Výstup příkazu ping v prostředí Windows Vista

Otázky, úkoly

- Prostuduj nápovědu ke zde uvedeným příkazům.
- Vyzkoušej si zde uvedené příkazy.

Další zdroje ke studiu

- Sítě v linuxu http://www.linuxsoft.cz/article.php?id_article=302

Použité obrázky

[1] Autorem je Vojtěch Novotný

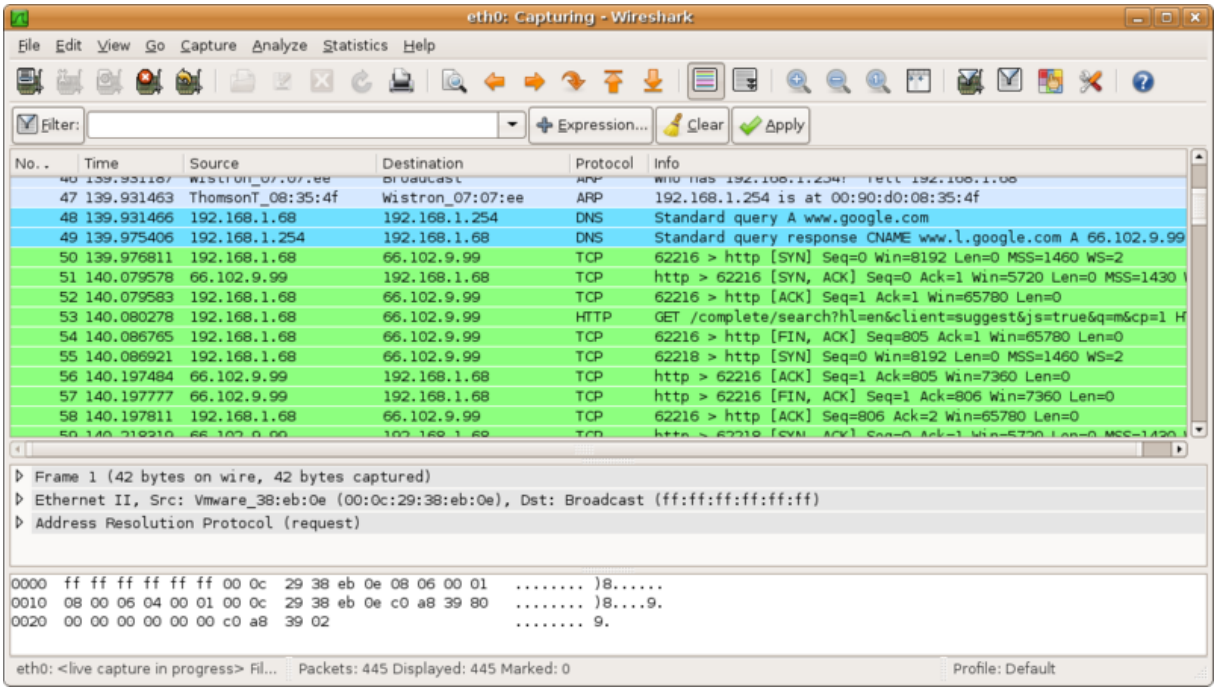
59. Síťové karty v promiskuitním režimu

Promiskuitní režim, je speciální režim síťové karty, ve kterém síťová karta předává nadřízené vrstvě nejen rámce s jí příslušející MAC adresou, ale i všechny ostatní zachycené rámce.

Do promiskuitního režimu lze kartu softwarově přepnout. Tato funkce je zpravidla integrována do specializovaných aplikací - tzv. slídících programů ("packet sniffer") neboli síťových analyzátorů ("network analyzer").

Známé síťové analyzátory jsou Wireshark (dříve Ethereal) nebo tcpdump.

Přepnutí síťové karty do promiskuitního režimu v podstatě znamená, že začneme odposlouchávat veškerý provoz na síti, který se dostane na rozhranní naší síťové karty. Pokud je to jednoduchá síť, kde jsou použity jen rozbočovače či mosty je možno odposlouchávat veškerý provoz. Pokud se v síti vyskytují přepínače či směrovače, tak ty již obsah filtrují podle toho, do kterého segmentu sítě jsou daná data určena. Existují ovšem i techniky jak donutit switche aby nám zasílali požadovaný obsah.



Obrázek 2. Okno programu Wireshark

59.1 Detekce síťových karet v promiskuitním režimu

Protože uživatel, který má síťovou kartu přepnutou do promiskuitního módu, představuje pro síť bezpečnostní riziko, vyvinuly se metody, jak detekovat v síti takovéto stanice.

Typy detekce:

- pomocí ARP paketů,
- pomocí ICMP echo paketů
- pomocí protokolu DNS,
- pomocí sledování odezvy.

59.2 Klamné segmenty sítě

Klamné segmenty sítě (návnada, "Honeypot"), jsou speciální segmenty sítě, které daná organizace nepoužívá a které obsahují klamné informace. Vnější firewall při detekci útoku umožní útočníkovi přístup do tohoto segmentu sítě. Ten zde pokračuje v útoku na jednotlivé prvky. Ztrácí tak čas a energii v útocích na bezcenné cíle a IDS systém současně získává cenné informace o útočníkovi a případně i o nových typech útoků.

Otázky, úkoly

Vyzkoušej si práci s programem Wireshark.

Další zdroje ke studiu

Použité zdroje

[1] BURDA, Karel, doc. Ing. CSc. *Návrh, správa a bezpečnost počítačových sítí*. FEKT VUT v Brně, Brno 2007.

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-24-08]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Wireshark_screenshot.png>.

60. Wireshark

Wireshark je "sniffovací" nástroj pro zachytávání a podrobnou analýzu veškeré síťové komunikace. Aplikace umí přepnout síťovou kartu do promiskuitního režimu a díky tomu dokáže zachytávat veškerou komunikaci na připojeném médiu. Program je přímým nástupcem aplikace Ethereal. Zachytávat je možno pakety procházející přes rozhraní. Aplikace je multiplatformní, takže ji lze provozovat na většině nejrozšířenějších operačních systémů.

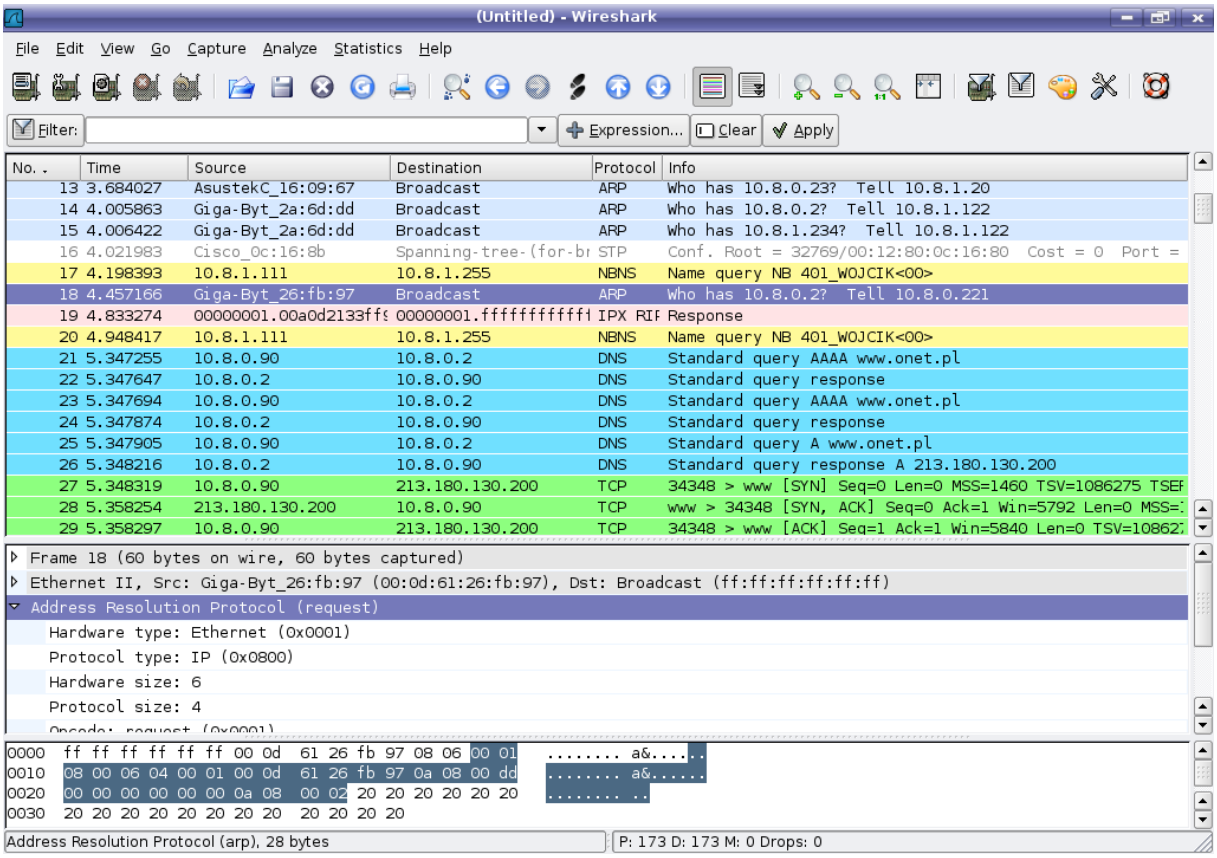
Obrázek 1. logo Wireshark

60.1 Vlastnosti

Wireshark je software, který rozumí struktuře různých síťových protokolů. Díky tomu je schopen zobrazit zapouzdření a další pole i s jejich významy pro různé pakety odlišných protokolů.

Data mohou být zachycena přímo z "drátu" živé sítě nebo přečtena ze souboru, kde jsou již zachycené packety zaznamenány.

- Zachytávat se může z několika typů sítí, jako je Ethernet, IEEE 802.11, PPP, loopback, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI a další
- Zachycená data mohou být procházena pomocí GUI, nebo v terminálové (příkazový řádek) verzi
- Zobrazení dat může být vylepšeno pomocí filtrů.
- Mohou být vytvořeny pluginy pro rozebírání nových protokolů.



Obrázek 2. Okno programu Wireshark

60.2 Práce s Wiresharkem

Wireshark pracuje pouze pasivně – neodesílá nic z vašeho počítače, pouze sleduje veškerý provoz, který je schopen zachytit.

Pokud Wireshark spustíte, objeví se před vámi menu, ve kterém si vybereme položku Interface List – kde jsou dostupné síťové rozhranní vašeho počítače, na kterých můžete zachytávat a analyzovat síťovou komunikaci. Tlačítkem start se začne zachytávat síťový provoz.

Před vámi se začnou vypisovat jednotlivé zachycené pakety, pokud nezačnou, tak je třeba nějakou vaší aktivitou (odesíláním či stahováním dat) nějaký data vygenerovat. V horní části okna, se vypisují pakety, které se standardně řadí podle času (Time), který je zobrazen jako druhý zleva hned za číslem paketu – No. Dále je zde IP adresa od koho byl paket poslán – Source a IP adresa příjemce – Destination. Následuje typ protokolu a dále základní informace o paketu. Pod tím následuje další okno, ve kterém se zobrazují podrobnější informace o paketu, který byl z horní nabídky vybrán. Ještě více dole jsou zobrazeny data, která přímo putují po síti. Abyste se vyznali ve velkém množství zachycených dat, lze data efektivně filtrovat.

60.3 Filtry

Filtry umožňují např. odchytávat pakety jenom od určité IP adresy.

Kliknutím na Capture v horní části menu a zadáním stop ukončíte skenování síťového provozu. Dále klikněte na tlačítko Options. Zde se nastavují filtry. Klikněte na Capture Filter a zde vyberte položku „IP address“ 192.168.0.1 a tu zaměňte na adresu, kterou chcete skenovat. Vedle tlačítka Capture Filtres, kde se nastavují filtry pro skenování, si můžete nastavit svůj vlastní filtr a to pomocí základní Booleovy algebry. Můžete také odchytávat jen data určitého provozu nebo odchytávat pakety, které obsahují určité textově řetězce (Pass).

Wireshark obsahuje ještě druhý způsob filtrování – Analýzu zachycených dat. Tento filtr nabízí větší možnosti než Capture filtres a najdete ho na horním, panelu pod položkou Analyze → Display filtres. Zde je trošku jiné nastavení výrazů, než v Capture filtres, ale pro pochopení a ukázku je zde na výběr pár výchozích výrazů, ze kterých si můžete vybrat a poté pomocí operátorů poskládat v textovém poli Filter string vlastní filtr. Zde je základní seznam operátorů, které se podobají operátorů v programovacím jazyce C, které se pro toto filtrování dají použít == – Rovná se, != nerovná se, && log. AND, || – log. OR .

Otázky, úkoly

- Nainstlauj a vyzkoušej si práci s programem Wireshark

Další zdroje ke studiu

- Průvodce progamem Ethereal (Wireshark) na root.cz: http://www.root.cz/serialy/pruvodce-programem-ethereal/

Použité zdroje

[1] Přispěvatelé Wikipedie, Wireshark [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 7. 04. 2012, 21:23 UTC, [citováno 16. 05. 2012] <http://cs.wikipedia.org/w/index.php?title=Wireshark&oldid=8363276> >

Použité obrázky

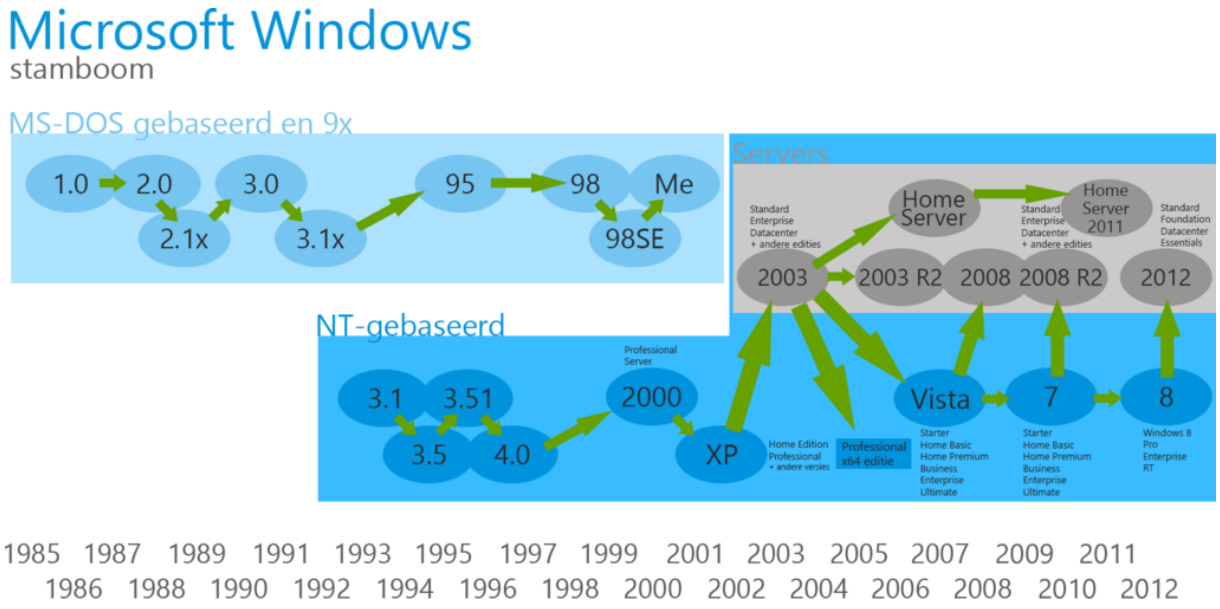
[1] Commons.wikimedia.org [online]. [cit. 2012-05-16]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Wsicon.svg?uselang=cs>.

[2] Commons.wikimedia.org [online]. [cit. 2012-05-16]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Ethereal_Screenshot.png?uselang=cs>.

61. Síťové operační systémy

Síťový operační systém (NOS) je software pro řízení provozu sítě a poskytování síťových služeb.

Síťových OS existuje celá řada např.:



Obrázek 1. Vývoj OS z rodiny Windows

Firma Microsoft
Windows server 2000, 2003, 2008, 2008 R2, 2012

Unixové systémy
AIX - unix firmy IBM
IRIX - unix firmy Silicon Graphic
HP-UX - unix firmy Hewlett-Packard
NOS Unixového typu
Linux
NetBSD
Solaris

Firma Novell
Novell NetWare 3.x, 4.x, 5.x, 6.x
Novell Open Enterprise Server na systému Linux

Poskytované služby

Síťové operační systémy oproti normálním operačním systémům poskytují rozšířené síťové služby. Zejména jsou to:

- doménové služby - správa zásad zabezpečení skupin
- tiskový server - poskytování a sdílení tiskáren
- databázový server - organizace a sdílení databází
- připojení sítě do internetu - Proxy server nebo paketový filtr
- souborový server - poskytování a sdílení diskového prostoru
- firewall - antivirové a bezpečnostní služby, ochrana proti průniku
- webový server - podpora www prezentací a aplikací
- poštovní server - správa elektronické pošty
- DHCP, DNS server - přidělování IP adres klientů a překlad jmen

61.1 Active directory

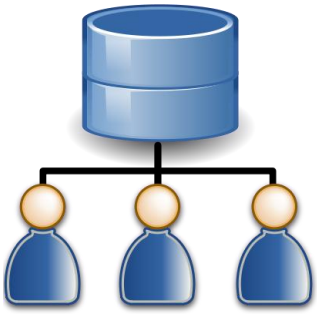
Active Directory je implementace adresářových služeb LDAP (Lightweight Directory Access Protocol) firmou Microsoft pro použití v prostředí systému Microsoft Windows. Active Directory umožňuje administrátorům nastavovat politiku, instalovat programy na mnoho počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře. Active Directory ukládá své informace a nastavení v centrální organizované databázi.

AD v sobě zahrnuje řadu služeb. Jeho primární role je poskytování centrálních služeb pro autentizaci a autorizaci, tedy ***správa uživatelů*** (přesněji správa účtů, protože to může být i třeba počítač). Ale různé části poskytují mnoho dalších funkcí, například ***Group Policy*** umožňuje spravovat politiky jednotlivých počítačů (co je na nich povoleno) a instalovat hromadně (a vzdáleně) aplikace.

AD je silně provázáno s **DNS**. AD používá stejnou hierarchickou strukturu jako DNS.

Tvorba a nastavení se provádí pomocí nástroje **Uživatelé a počítače služby Active Directory.**

Uživatelé v AD nemají žádnou souvislost s uživateli vytvořenými na lokálních stanicích.



Obrázek 2. Active directory

Profil uživatele
Přihlašovací údaje včetně pravidel
Nastavení domovských adresářů
Členství ve skupinách a kontejnerech
Připojení síťových disků, tiskáren a dalších
Diskové kvóty
Vzdálené řízení a terminálové služby
Uživatelské prostředí

Skupinové zásady
umožňují nastavit a upravovat profily skupin uživatelů
učitelé - možnost instalace aplikací
žáci - zákaz čtení a zápisu z USB
hosté - omezený přístup k síťovým diskům
zařazením uživatel ke skupině dojde k uplatnění skupinových zásad

Otázky, úkoly

Další zdroje ke studiu

Vývoj OS Windows
http://www.fd.cvut.cz/personal/xfabera/SSS/prednasky/Win_predn1.pdf

Použité zdroje

[1] Přispěvatelé Wikipedie, Active Directory [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 27. 04. 2012, 07:23 UTC, [citováno 24. 07. 2012] <http://cs.wikipedia.org/w/index.php?title=Active_Directory&oldid=8460451>

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-05-16]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Windows_Tijdlijn.png>.

[2] Commons.wikimedia.org [online]. [cit. 2012-05-16]. Dostupný pod licencí Public domain na WWW: < http://commons.wikimedia.org/wiki/File:Active-directory.svg>.

62. OS Linux

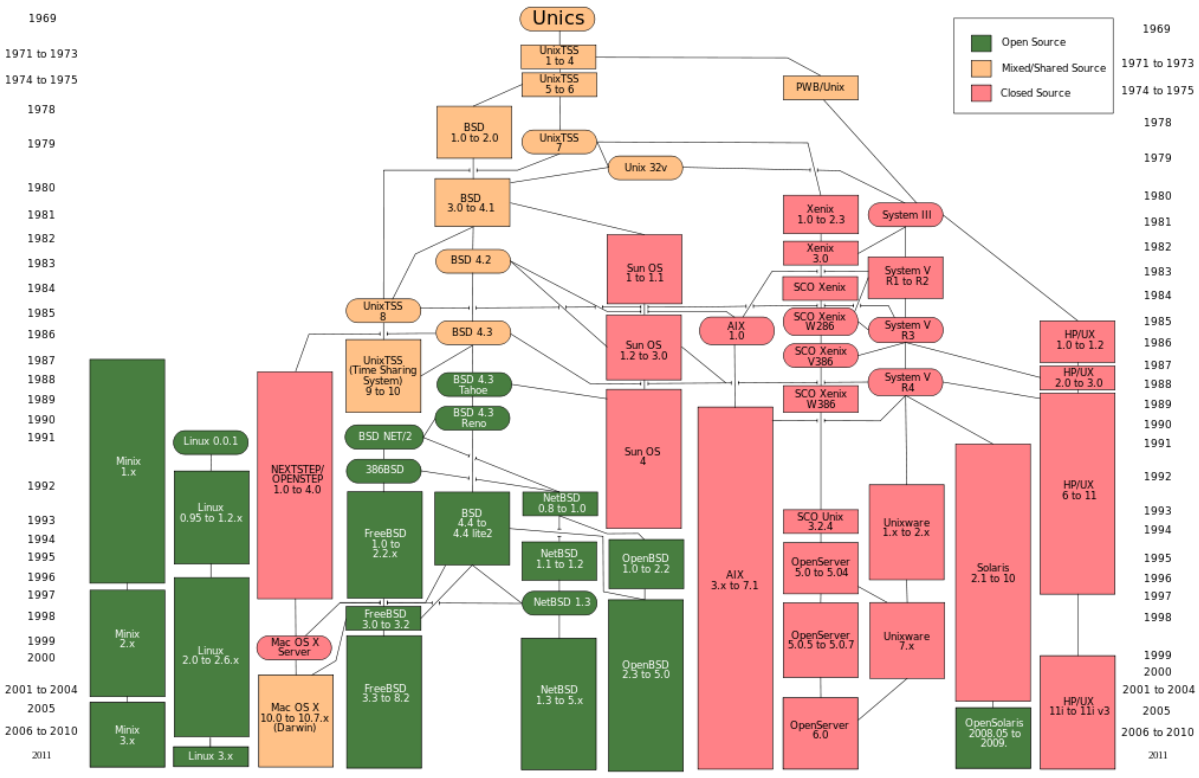
Vlastnosti Linuxu

Charakteristika

- volně šířený operační systém vycházející z Unixu
- modulární monolitické jádro programované v jazyce C
- autorem Linus Torvald - v roce 1991 student univerzity v Helsinkách
- dnes dohlíží na vývoj podporovaný komunitami programátorů i firem - Intel, IBM

Vývoj jádra

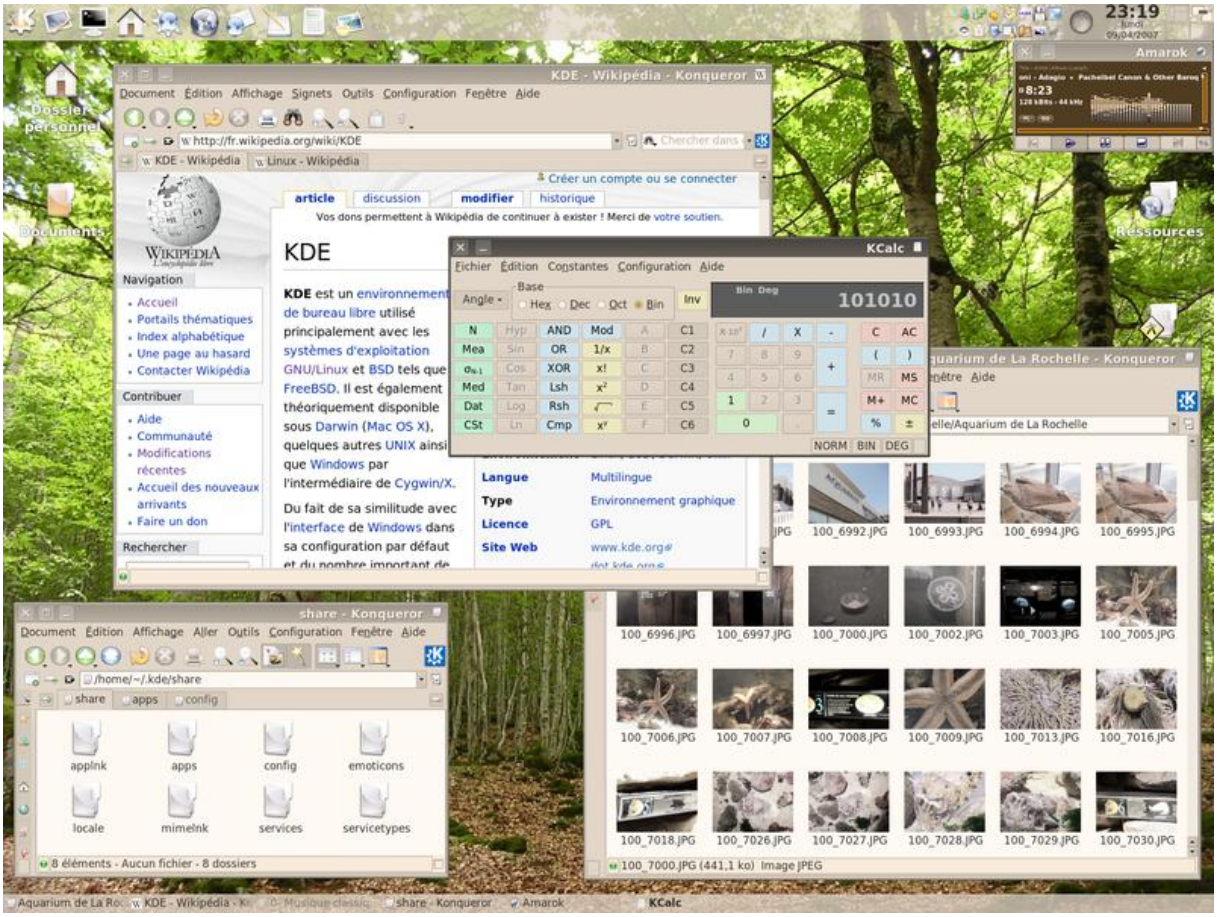
- 1991 - 0.0.1 - 10 000 řádků kódu
- 1994 - 1.0.0 - 200 000 řádků kódu
- 1996 - 2.0.0 - 800 000 řádků kódu
- 2003 - 2.6.0 - 6 000 000 řádků kódu
- 2011 - 2.6.39 - 15 000 000 řádků kódu



Obrázek 1. Vývoj Unixových systémů

Distribuce - odladěná sestava OS(GPL) a SW(GNU)
jádro OS Linux + systémové knihovny + dokumentace
grafické rozhraní + programové aplikace

Nejpoužívanější - Ubuntu, Mandriva, Debian, Suse, Fedora, RedHat



Obrázek 2. Linux s rozhranním KDE

Rozdělení

- Podle počítačové platformy - PC Intel(32/64bit), PC Mac
- Podle grafického rozhraní - X-Win, X-Fce, GNOME, KDE
- Podle instalace - Live CD, Mini CD, Full DVD

Ovládání a nastavení je možno buď v grafickém rozhranní nebo častěji efektivněji pomocí konzoly v textovém režimu.

Práce s konzolou

- textové rozhraní pro ovládání Linuxu pomocí příkazové řádky
- spolupráce s interpreterem příkazů - Shell

- možnost víceuživatelského přístupu - 6x textových terminálů
- možnost spuštění v grafickém režimu - aplikace **Terminál**
- pro konfiguraci a instalaci služeb a systémových aplikací
- pro vzdálené ovládání a konfiguraci síťových služeb

Základní příkazy

adresáře – dir (výpis), tree (struktura), cd (změna), mbir (vytvoření), rmdir (smazání)

soubory - ls (výpis), cp (kopie), mv (přesun), rm (smazání)

systém – useradd (přidání už.), userdel (smazání už.), chmod (oprávnění)

Grafické rozhraní

Několik základních typů grafického uživatelského rozhranní GUI - GNOME, KDE, X-WIN

Souborové systémy

ext - Extended Filesystem - **ext4** od roku 2007- max. soubor 1 TB (tera 1.10^{12}), max. disk 1 EB (exa 1.10^{18}), podpora FAT a NTFS

Adresářová struktura

/ - kořenový adresář celé struktury
/bin - systémové příkazy Linuxu
/dev - soubory zařízení
/etc - konfigurační soubory s nastavením systémových příkazů
/home - domovské adresáře jednotlivých uživatelů
/mnt - připojeny jako podadresáře ostatní disky
/root - domácí adresář uživatele root (administrátora)
/usr - nainstalované aplikační programy

Diskové jednotky

hd - disk na IDE rozhraní
sd - disk na SATA, USB (SCSI) rozhraní
/dev/sda - první disk
/dev/sdb - druhý disk

Diskové oddíly

4 primární (systémové log. disky) - **/dev/sda1** - /dev/sda4
4 rozšířené (datové log. disky) - **/dev/sda5** - /dev/sda8

Software pro Linux

Způsob instalace
repozitáře - internetové servery se softwarovými balíčky pro distribuce
správce balíčků - systém pro stahování a instalaci softwaru pro Linux

Kancelářské aplikace
Open Office, KOffice, Gnome Office, AbiWord, Acrobat Reader

Grafické editory
Gimp, XnView, InkScape, Blender, DraftSight

Otázky, úkoly

- Vyzkoušej si práci v OS Linux.
- Vyhledej co nejvíce různých distribucí Linuxu.
- Zkus si vyrobit „záchraný disk“ s OS Linux

Další zdroje ke studiu

- Linux na Wikipedii http://cs.wikipedia.org/wiki/Linux

Použité zdroje

[1] Wikipedie: Otevřená encyklopedie: Linux [online]. c2012 [citováno 24. 08. 2012]. Dostupný z WWW: <http://cs.wikipedia.org/w/index.php?title=Linux&oldid=8822793>

Použité obrázky

[1] Commons.wikimedia.org [online]. [cit. 2012-05-16]. Dostupný pod licencí Public domain na WWW: <http://commons.wikimedia.org/wiki/File:Unix_history-simple.svg>.

[2] Commons.wikimedia.org [online]. [cit. 2012-05-16]. Dostupný pod licencí Public domain na WWW: <http://commons.wikimedia.org/wiki/File:Kde_3.5.5_-_004.png>.

63. Test

1./10 Kolik vrstev má referenční model iso/osi?
4
6
7

2./10 Co je to resolver?
Komponenta systému zabývající se překladem ip adresy
Systém doménových jmen
Zesilovač signálu, přijímá zkreslený signál a vysílá ho dále opravený, zesílený

3./10 Co je to csma/ca?
Přístupová metoda, kterou se rezervuje kanál pro přenos
Program pro lokální doručování, který umisťuje zprávy do uživatelských schránek
Oblast pokryta jedním Access Pointem

4./10 Z které specifikace vychází standard Wifi?
i e e e 804.11
i e e e 803.11
i e e e 802.11

5./10 Na které vrstvě iso/osi modelu pracují protokoly ip, icmp, arp, rip?
Na linkové vrstvě
Na síťové vrstvě
Na transportní vrstvě

6./10 Co je to mta (mail transfer/transport agent)?
Poštovní klient, který zpracovává zprávy u uživatele
Server, který se stará o doručování zprávy na cílový systém adresáta
Program pro lokální doručování, který umisťuje zprávy do uživatelských schránek, případně je může přímo automaticky zpracovávat

7./10 Co znamená zkratka ad v síti Microsoft klient-server?
Active Directory
Asymmetric Database
Allocation Database

8./10 Co je to Ping of Death?
Paket, který se ztratil při cestě k cíli
Nic takového v počítačové terminologii neexistuje
Paket je větší než maximálně možný a způsobí zpravidla zhroucení systému

9./10 Co je to dmz (demilitarized Zone)?
Segment sítě umístěný mezi vnitřní a vnější sítí
Zóna, ve které spolu sdílejí data firmy jako ibm, Microsoft, Apple a další
Zóna neboli karanténa, do které se mohou přesunout nalezené viry v počítači

10./10 k čemu slouží arp paket?
k získání ip adresy daného pc v síti z jeho ethernetové (mac) adresy
k získání ethernetové (mac) adresy daného

Otázka 1.:
Anglicky počítačová síť?
a) netstation
b) network
c) internet
d) site

Otázka 2.:
V které síti mají počítače rovnocenné postavení?
a) klient-server
b) Linux
c) peer-to-peer
d) net-net

Otázka 3.:
Který operační systém není síťový?
a) MS DOS
b) UNIX
c) LINUX
d) Windows NT

Otázka 4.:
V které síti je přenosová rychlost kbps?
a) LAN
b) MAN
c) WAN
d) WWW

Otázka 5.:
Která komponenta umožňuje propojit dva počítače?
a) grafická karta
b) síťová karta
c) procesor
d) MAC

Otázka 6.:
10Base2 je označení...
a) TP
b) USB
c) koaxiálního kabelu
d) pro LAPlink

Otázka 7.:
Elektromagneticky nelze rušit kabel...
a) optický
b) koaxiální
c) kroucenou dvoulinku
d) žádný

Otázka 8.:
Rychlost 10Mb/s dosahujeme u ...
a) rádiového přenosu
b) optického přenosu
c) mikrovlnného přenosu
d) SCSI rozhraní

Otázka 9.:
Při přerušení HUbu v topologii STAR síť
a) přestane fungovat
b) nepřestane fungovat
c) přestane fungovat jen 1 počítač
d) přestane fungovat server

Otázka 10.:
Technologii Token Ring nalezneme jen u topologie
a) STAR
b) Ring
c) BUS
d) libovolné

Otázka 11.:
Zesilovat signál v síti umožňuje
a) Bridge
b) Gateway
c) BUS
d) Repeater

Otázka 12.:
Fyzická adresa síťové karty má označení
a) Adress
b) IP
c) MAC
d) DNS

Otázka 13.:
Nejefektivnější cestu v síti vyhledá
a) Router
b) Bridge
c) Gateway
d) Hub

Otázka 14.:
IP adresa má...
a) 32 bitů
b) 18 bitů
c) 8 bitů
d) 64 bitů

Otázka 15.:
DNS server
a) umožňuje procházet internetové stránky
b) automaticky nastaví IP adresu počítačů v síti
c) umožňuje pracovat se soubory vzdáleného počítače
d) převádí IP adresu na jméno uzlu

Otázka 16.:
Komunikační protokol pro odesílání pošty se jmenuje
a) POP3
b) SMTP
c) HTML
d) HTTP

Otázka 17.:
Program pro přenášení souborů síťového serveru se jmenuje
a) Word
b) Seznam
c) CuteFTP
d) FTP

Otázka 18.:
Program pro hlasovou komunikaci se jmenuje
a) NetMeeting
b) FrontPage
c) MSWorks
d) MS Speak

Otázka 19.:
WWW je zkratka
a) World Wide Web
b) Word Wide Web
c) Web Web Web
d) Wery Wide Web

Otázka 20.:
Vyberte nesprávnou adresu:
a) www.škola.cz
b) www.www.skola.cz
c) skola.cz
d) skola.cz.

Otázka 21.:
Uveďte topologie sítě kdy komunikace probíhá jedním směrem a signál se neztrácí
a) STAR
b) RING
c) BUS
d) žádná

Otáz 22.:
Které zařízení nelze použít v síti jako centrální prvek
a) modem
b) Hub
c) Router
d) Bridge

Otázka 23.:
Jakým příkazem zjistíte MAC adresu síťového adaptéru?
a) ping
b) ipconfig/all
c) ipconfig
d) command

Otázka 24.:
Protokol pro automatické přidělování IP adres pracovním stanicím se jmenuje
a) IMAP
b) DNS
c) DHCP
d) FTP

Otázka 25.:
U mikrovlnného přenosu lze dosáhnout rychlosti
a) přesně 150 Mb/s
b) maximálně 10 Mb/s
c) menší než 100 Mb/s
d) větší než 100 Mb/s

Otázka 26.:
Terminátor je ...
a) zakončovací odpor u koaxiálního kabelu
b)centrální síťový prvek
c) název pro UTP konektor
d) zakončení UTP kabelu

Otázka 27.:
Protokol pro čtení e-mailů se jmenuje ...
a) POP3
b) IMAP
c) SMTP
d) FTP

Otázka 28.:
U koaxiálního kabelu měříme odpor v Ohmech
a) 50
b) 25
c) 100
d) 10

Otázka 29.:
Označte nepravdivé tvrzení:
a) technologie TokenRing je pomalejší než Ethernet
b) Switch je Hub, který přenáší data tam, kam patří
c) IMAP je protokol pro přijímání mailů mimo lokální počítač
d) UTP kabel je pro vzdálenost maximálně 100 m

Otázka 30.:
Jakým příkazem zjistíte dostupnost počítače se jménem Cislo3
a) ipconfig Cislo3
b) ping
c) ping Cislo3
d) ping 193.60.1.3

Otázka 31.:
Síťový prvek, který propojuje 2 sítě s různými topologiemi se jmenuje...
a) Router
b) Bridge
c) Hub
d) Gateway

Otázka 32.:
Protokol pro vzdálenou správu počítače se jmenuje...
a) http
b) DHCP
c) DNS
d) telnet

Otázka 33.:
Server, který spravuje poštovní služby na síti se označuje...
a) Mail server
b) FTP server
c) Fax server
d) Print server

Otázka 34.:
Program pro prohlížení internetových stránek se jmenuje
a) Netmeeting
b) FrontPage
c) Explorer
d) CutFtp

Otázka 35.:
Síť na kilometrové vzdálenosti se jmenuje
a) LAN
b) VAN
c) MAN
d) WWW

Otázka 36.:
Virtuální místnost pro textovou komunikaci po Internetu se označuje jako
a) chat
b) www
c) room
d) text room

Otázka 37.:
UTP je pro
a) optický kabel
b) stíněnou kroucenou dvoulinku
c) koaxiální kabel
d) nestíněnou kroucenou dvoulinku

Otázka 38.:
První síťový předchůdce Internetu se jmenoval
a) Junet
b) Gopher
c) Damis
d) Arpanet

Otázka 39.:
Mikrovlnný přenos vyžaduje
a) nastavenou určitou frekvenci
b) paraboly, které nemusí být přesně nařízené
c) paraboly přesně nařízené
d) optické kabely

Otázka 40.:
Mezi technologie bezdrátového připojení nepatří
a) IrDA
b) Bluetooth
c) WiFi
d) USB

1. Kolik vrstev uvažuje model ISO/OSI ?
Nápověda: fyzickou, linkovou ...
3
4
7

2. TCP/IP - s kolika vrstvami síťového programového vybavení počítá ?
4
7
3

3.
K čemu slouží protokol ICMP ?
k nastavování síťových prvků
podpora a kontrola skupinových vysílání
k informování o nestandardních situacích = posel špatných zpráv

4.
K čemu slouží POP3 ?
ke čtení pošty uložené na serveru
ke stahování pošty
k odesílání pošty

5.
K čemu slouží SMTP ?
k ničemu
ke čtení emailů
k odesílání emailů

6.
K čemu slouží RPC ?
ke správě síťových prvků
ke vzdálenému volání procedur
k potvrzování emailů

7.
Rozdíl mezi TCP a UDP ?
UDP se používá pro internet a TCP pro lokální sítě
komunikace přes TCP je potvrzovaná a spolehlivá, UDP je nespolehlivé
UDP vytváří virtuální kanály a proto se nedá odposlouchávat, TCP ano

8. Jaký je rozdíl mezi FTP/TFTP ?
TFTP nepodporuje autorizaci a např. prohlížení adresářů, FTP ano
FTP nepodporuje autorizaci, TFTP ano
žádný, je to skoro to samé, jen TFTP je šifrované

1. Veřejné počítače jsou
k dispozici v knihovně, kavárně, letišti apod.
všechny na trhu dostupné notebooky
firemní počítače spravované jedním správcem

2. Veřejný počítač může používat
kdokoli
jen evidovaný uživatel
jen člen určité sociální skupiny

3. Při použití veřejného počítače přihlašovací či citlivé údaje
zapíši do knihy návštěv
nahlásím obsluze počítače
nikdy neukládám do daného počítače

4. Brána firewall
umožňuje rychlou aktualizaci antivirového programu
zabraňuje vypnutí počítače po dobu dvou hodin
pomáhá zabránit počítačovým podvodníkům nebo škodlivému softwaru (například červům) v získání přístupu k počítači

5. Připojení k bezdrátové síti
je veřejné i domácí PC naprosto bezpečné
je domácí PC naprosto bezpečné, zato u veřejného může hrozit bezpečnostní riziko
může u domácího i veřejného PC dojít k napadení škodlivým softwarem

6. Používat internetbanking či platby kartou na internetu není vhodné
na veřejném počítači
na soukromém notebooku
na domácím počítači

7. Po skončení práce na veřejném počítači
vymaži všechny dostupné soubory a programy
neukládám žádné soubory ani data, navíc odstraním v prohlížeči historii procházení
uložím si svoji práci a počítač vypnu

8. Ke zvýšení ochrany přenosu souborů na veřejných bezdrátových sítích se používá
zipování
šifrování
zálohování na externí disk

9. Při používání veřejné bezdrátové sítě z důvodu bezpečnosti
nezadávám čísla kreditních karet ani hesla
při zadávání osobních údajů si chráním klávesnici tak, aby nikdo neviděl, co zadávám
mohu zadávat libovolné údaje, protože veřejná bezdrátová síť je bezpečná

10. Jak se sníží riziko napadení počítače útočníkem prostřednictvím veřejné bezdrátové sítě?
vypnutím připojení k bezdrátové síti, když ji nepoužívám
pravidelným zálohováním dat
vypnutím brány firewall

1. K čemu slouží IP adresa?
a. zajišťuje internetovou telefonii
b. k jednoznačné identifikaci PC v počítačové síti
c. k připojení vypalovací mechaniky
d. k výběru internetového prohlížeče

2. Co označuje pojem spam?
a. e-maily přicházející z adres, které jsou již uloženy v adresáři
b. antivirovou kontrolu poštovních zpráv
c. poštovní program
d. nevyžádanou poštu

3. Převod doménového jména na IP adresu počítače a naopak zajišťuje:
a. FTP
b. TCP/IP
c. DNS
d. http

4. Doména nejvyššího řádu České republiky má přiděleno označení:
a. cs
b. Czech republic
c. cz
d. com

5. Doménu nejnižšího řádu si může v rámci České republiky zaregistrovat:
a. kdokoliv
b. pouze občan České republiky
c. pouze občan České republiky nebo Slovenska
d. člověk s trvalým bydlištěm v rámci hranic Evropské unie

6. Znak @ (zavináč) obsahuje jako povinnou součást jednoznačného určení služba:
a. e-mail
b. VOIP
c. FTP
d. https

7. Internetová služba WWW vznikla:
a. v 90. letech 19. století
b. v 70. letech 20. století
c. v 90. letech 20. století
d. na počátku 21. století

8. Která z uvedených zkratek neoznačuje žádnou z internetových služeb?
a. VOIP
b. HTML
c. WWW
d. FTP

9. Vyberte z nabízených názvů ten, který neoznačuje žádný z webových prohlížečů?
a. Opera
b. Microsoft Internet Explorer
c. Mozilla Firefox
d. Total Commander

10. Protokol zajišťující provoz elektronických služeb na mobilních telefonech má zkratku:
a. WAP
b. Google
c. Firefox
d. XML

11. Který z uvedených způsobů připojení k Internetu poskytuje nejnižší přenosovou rychlost?
a. Wi-Fi
b. ADSL
c. ISDN
d. Dial-up

12. HTML je značka pro:
a. jazyk pro vytváření webových stránek
b. přenosový protokol
c. jednoznačný identifikátor v počítačové síti
d. webový prohlížeč

13. Kontrolu bezchybného zápisu HTML stránky lze ověřit pomocí:
a. webového prohlížeče
b. validátoru
c. OS Windows Vista
d. poštovního klienta

14. Webová stránka, v jejímž zdrojovém kódu se vyskytuje chybně zapsané formátovací značky, se ve webovém prohlížeči:
a. nezobrazí
b. zobrazí, ale zasláno chybové hlášení společnosti Microsoft
c. webový prohlížeč se stránku pokusí zobrazit vždy
d. zobrazí jen se speciálním doplňkem výbavy webového prohlížeče

15. JavaScript patří do skupiny:
a. programovacích jazyků
b. webových prohlížečů
c. grafických editorů
d. operačních systémů

16. Která z následujících přípon slouží pro označení souboru webové stránky?
a. *.gif
b. *.doc
c. *.jpg
d. *.htm

64. Přílohy

Slovníček pojmů

Access point – zkráceně AP – česky přístupový bod. Jedná se o zařízení, které je prostředníkem v bezdrátových Wi-Fi sítích. Umožňuje nepřímou komunikaci mezi klienty.

ADSL – Asymmetric Digital Subscriber Line – asymetrické digitální účastnické vedení po stávajícím telefonním vedení.

Anycast – Pojem pro výběrové směrování a adresy. Anycast adresu může mít více zařízení najednou, ale paket bude doručen pouze na to nejbližší.

ARPANET Advanced Research Projects Agency Network – počítačová síť, kterou lze označit za předchůdce dnešního internetu.

Baud – Bd - jednotka přenosové rychlosti. Bd = 1 bit/s.

Bitrate – Datový tok - udává se nejčastěji v kb/s nebo Mb/s (též kbps nebo Mbps)

Bluetooth – bezdrátová komunikační technologie, 2,4GHz pásmo, 720 kbps.

BNC – Bayonet Locking Connector - konektor s bajonetovým zámkem.

Bridge – Most (z angl. bridge) je síťové zařízení, pracující na linkové vrstvě.

Broadcast – Všesměrové vysílání (všem uzlům v daném segmentu sítě).

Browser – prohlížeč, program, který zobrazuje dokumenty, zveřejněné na Internetu.

BSD – *Berkeley Software Distribution*. Používáno v souvislosti s operačními systémy typu *Unix* (*FreeBSD, OpenBSD* apod.).

Byte – Bajt (označení velkým písmenem "B"). V běžné počítačové praxi se velmi často setkáme s odvozenými jednotkami: 1 KB (kilobyte) = 1 024 B (velké "K" je zvoleno záměrně, protože zde nemluvíme o násobku 1 000); 1 MB (Megabyte) = 1 048 576 B; 1 GB (Gigabyte) = 1 073 741 824 B; 1TB (Terabyte) = 1 099 511 627 776 B. Toto je obvyklý způsob značení, avšak s platností od 1. dubna 2004 byl v Česku přijat nový standard, který byl již dříve schválen mezinárodní elektrotechnickou komisí IEC, a který mění binární předpony. Správně by se nyní mělo 1024 bajtů zapisovat jako 1 KiB (kibibyte), přičemž 1 kB má označovat pouze rovných 1 000 bajtů (správně tedy již s malým "k", neboť se jedná o násobek 1 000), tak jak je tomu zvykem v soustavě SI. Nově bychom tedy měli používat také mebibyte (MiB), gibibyte (GiB) a tebibyte (TiB).

DHCP – *Dynamic Host Configuration Protocol*. Konfigurační protokol, který umožní ze serveru získávat klientům základní konfigurační informace o jejich adrese, výchozí bráně a podobně.

DNS – *Domain Name System*. Systém doménových jmen. Internetový systém umožňující překládat číselné adresy na jména a naopak.

Download – "stažení" souboru.

Ethernet – Nejpoužívanější síťová technologie fyzické a linkové vrstvy v lokálních sítích.

FAQ – *Frequently Asked Questions* – Často kladené dotazy.

Firewall - je bezpečnostní brána, která definuje pravidla komunikace mezi sítěmi.

FTP – *File Transfer Protocol*. Jeden z protokolů založených na *TCP/IP*, sloužící k přenosu souborů mezi dvěma uzly.

GUI – *Graphical User Interface.* Grafické uživatelské rozhraní.

HTML – hypertext markup language – hypertextový značkovací jazyk.

HTTP – *Hypertext Transfer Protocol*. Jeden z protokolů založených na *TCP/IP*, sloužící k přenosu hypertextového obsahu, nejčastěji pak stránek systému *WWW*.

Hypertextový odkaz – jedná se o určitou část dokumentu, například text nebo obrázek, který odkazuje na jiný dokument nebo jeho část. V internetovém prohlížeči se uživatel po kliknutí na odkaz přenese na příslušný odkazovaný dokument.

ICMP – Internet Control Message Protocol je povinný standard TCP/IP a vyžadovanou součástí IP protokolu. Umožňuje strojům využívající IP komunikaci ohlašovat chyby a jejich příčiny.

IEEE – *Institute of Electrical and Electronic Engineers*. Standardizační instituce v oblasti elektroniky a také výpočetní techniky.

IETF – *Internet Engineering Task Force*. Organizace neformálně sdružující řadu pracovních skupin, které se podílí na vývoji Internetových standardů.

IP – Internetový protokol. Standard síťové vrstvy v rozlehlých sítích.

IPv4 – IP verze 4. V současnosti používaná verze *IP* protokolu. Vizte IP.

IPv6 – IP verze 6. Nástupce *IPv4* protokolu.

ISO – Mezinárodní organizace pro normalizaci. Tato organizace se primárně zabývá tvorbou mezinárodních norem ISO.

LINUX – **GNU/LINUX** – Operační systém *unixového* typu vyvíjený s otevřeným zdrojovým kódem.

MAC adresa – (*Media Access Control*) – Jedinečný identifikátor síťového zařízení, na druhé (spojové) vrstvě modelu OSI. Je přiřazována síťovému prvku při jeho výrobě.

Masquerade – maškaráda – Překlad zdrojové adresy (*NAT*), kdy není zadáno, na jakou adresu se má překládat. Systém použije stejnou *IP* adresu, jakou má síťové rozhraní, ze kterého paket odchází.

Mobilita – Dosažitelnost prvku v případě jeho pohybu (změny umístění), a to pod stále stejnou adresou.

Modem – Zařízení, které moduluje/demoduluje signál o určité frekvenci.

Most – *Bridge* – Pracuje na druhé vrstvě *ISO-OSI* modelu. Most se používá k rozdělení kolizní domény, rozpozná jaký paket do daného segmentu sítě patří a jaký ne, tedy co nemusí, neposílá dál. Mosty byly v *Ethernet* sitích nahrazeny přepínači.

Multicast – Skupinové přenosy. Data se vysílají z jednoho zdroje více příjemcům najednou při šetření přenosového pásma.

NAT – *Network Address Translation*. Překlad *IP* adres (někdy *IP maškaráda*). Používá se k úspoře *IP* adres v Internetu. Většinou je realizován například na směrovači připojujícím lokální síť k internetu. V lokální síti mohou pak být použity libovolné adresy (nejčastěji adresy z neveřejného rozsahu).

OSPF – (Open Shortest Path First) je protokol používaný pro interní routování uvnitř autonomního systému (AS).

Paket – základní jednotka přenosu informace v počítačových sítích.

PoE – Power over Ethernet - Technologie, která popisuje distribuci elektrické energie k síťovým zařízením přes ethernetový kabel (CAT5 a vyšší).

Promiskuitní mód – Mód, kdy síťová karta nezahazuje pakety určené pro jinou adresu než má ona sama, ale zachytává je a umožňuje jejich další zpracování.

Protokol – předpis, který určuje způsob komunikace mezi počítači, zajišťuje uskutečnění přenosu: navázání, udržení a ukončení spojení

Přepínač – *Switch* – Síťový prvek druhé vrstvy *IP* protokolu.

QoS – *Quality of Services*. Obecně znamená možnost definovat kvalitativní a kvantitativní (např. šířku pásma) požadavky na poskytovanou službu – přenosový kanál.

RFC – *Request For Comments*. Dokument vydaný *IETF* upravující určitou oblast. Může jít o standard nebo informační text. Vzniká většinou jako konsenzus pracovních skupin *IETF*.

Router – česky směrovač. Jedná se o zařízení, které směruje (routuje) provoz v síti. Router pracuje většinou na síťové.

Server – bezobslužný program (nikoli tedy stroj) běžící na počítači permanentně zapojeném v počítačové síti, který nabízí služby dalším počítačům a serverům

Skok – *Hop* – Jedno směrování mezi dvěma uzly.

Směrovač – *Router* – Síťový prvek třetí vrstvy *IP* protokolu.

Směrování – *Routing* – Proces, kterým se podle cílové *IP* adresy v paketu určí další cesta, kudy je potřeba paket poslat.

Software – programové vybavení, jakýkoliv program (např. editor textů, internetový prohlížeč, elektronický slovník).

TCP – *Transmission Control Protocol*. Protokol transportní vrstvy bezprostředně související s IP a využívající jeho služeb. Jde o spojovaný přenos.

TCP/IP – Transmission control protocol / Internet protocol – protokol, dle kterého funguje komunikace v síti Internet.

UDP – *User Datagram Protocol*. Protokol transportní vrstvy bezprostředně související s *IP* a využívající jeho služeb. Jde o nespojovaný přenos.

Upload – termín používaný pro přenos dokumentu (souboru) z uživatelova počítače na internetový server (nebo jiný počítač).

URL – Uniform Resource Lokator – adresa umístění webové stránky (též internetová adresa; webová adresa).

VoIP – "Voice over Internet Protocol". Jedná se o technologii, která umožňuje přenos digitalizovaného hlasu prostřednictvím počítačové sítě.

W3C – World Wide Web Consorcium – mezinárodní organizace založená v roce 1994 stanovující standardy pro WWW.

WEP – Wired Equivalent Privacy - v překladu soukromí ekvivalentní drátovým sítím. Vzhledem k jeho nízké úrovni zabezpečení, označen jako překonaný.

WiFi – *Wireless Fidelity* – označení bezdrátových síťových prvků pracujících podle standardu 802.11x.

WiMax – (Worldwide Interoperability for Microwave Access) – jedná se technologii v oblasti bezdrátového připojení zaměřenou na venkovní sítě.

WWW – World Wide Web – zkratka pocházející z anglického WorldWide Web (v překladu celosvětová pavučina). Jedná se o jednu z nejužívanějších služeb Internetu, která nabízí k prohlížení „webové“ stránky. Charakteristickým rysem webu jsou tzv. hypertextové odkazy (odtud pavučina). Často se používá pouze zkrácený termín web.

Seznam obrázků

strana

obrázek klapky http://www.clker.com/clipart-15324.html

Seznam použitých zdrojů

[1] PŘISPĚVATELÉ WIKIPEDIE. [online], Wikipedia: Otevřená encyklopedie, [citováno 28. 8. 2008 – 1.9.2012] <http://en.wikipedia.org/ > a <http://www.wikipedia.cz/ >.

[2] MOLNÁR, Karol, ZEMAN, Otto. *Moderní síťové technologie laboratorní cvičení*, VUT v Brně, Fakulta elektrotechniky, Ústav telekomunikací, 2006. 91 s. <http://www.utko.feec.vutbr.cz/~molnar/MMOS/MMOS_lab.pdf>.

[3] PETERKA, Jiří. *Principy počítačových sítí* [online]. 1992 - 2008, [citováno 28. 8. 2008]. < http://www.earchiv.cz/i_serial.php3>.

[4] NOVOTNÝ, Vít, doc. Ing. Ph.D. *Architektura sítí*. FEKT Vysokého učení technického v Brně, Brno 2006.

[5] BURDA, Karel, doc. Ing. CSc. *Bezpečnost informačních systémů sítí*. FEKT Vysokého učení technického v Brně, Brno 1. 11. 2005.

[6] HERMAN, Ivo, Ing. CSc. *Komunikační technologie*. FEKT Vysokého učení technického v Brně, Brno 2006.

[7] MOLNÁR, Karol, Ing. *Praktikum z informačních sítí*, VUT v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Brno.