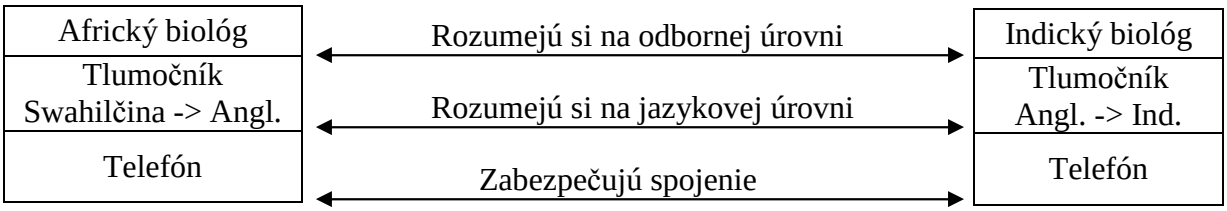
Komunikačné protokoly

Základným predpokladom na to, aby mohli dva počítače navzájom komunikovať, je ich vzájomné prepojenie do spoločnej siete, alebo navzájom prepojených sietí. Avšak ani tento fakt nezabezpečí, že počítače budú vedieť medzi sebou komunikovať. Je potrebné aby poznali a používali rovnaký komunikačný protokol. Počítač môže byť schopný komunikovať pomocou niekoľkých, súčasne inštalovaných protokolov. To zabezpečí väčšiu rýchlosť a priepustnosť (alebo bezpečnosť) siete. Ostáva ešte vyriešiť otázku, ako v sieti jednoznačne identifikovať konkrétny počítač, teda ako nadviazať spojenie s konkrétnym počítačom. Každý počítač je možné vzhľadom k použitému protokolu nakonfigurovať tak, aby bol v rámci siete jedinečný a teda identifikovateľný aj pre ostatné počítače. Samozrejme spôsob konfigurácie sa v závislosti od použitého protokolu líši. A to čo býva najlepšie, býva aj najťažšie konfigurovateľné.
Komunikačný protokol – súhrn parametrov a pravidiel, ktorými sa riadi komunikácia. Ide predovšetkým o druh prenosu, jeho rýchlosť, kontrolu apod. Aby mohlo dôjsť k úspešnej komunikácii musia obe strany dodržiavať daný komunikačný protokol.

Príklad:



Protokol – definuje, akým spôsobom sa odovzdávajú informácie medzi vrstvami

Základné komunikačné protokoly

Zameriame sa predovšetkým na siete MS (ale nie len na ne).

NetBEUI

Komunikačný protokol NetBEUI (NetBIOS Extended User Interface) bol vyvinutý firmou IBM v polovici 80. rokov 20. storočia.. Stal sa v podstate štandardom v prostredí malých sietí MS Windows. Často sa využíva pri komunikácií medzi pracovnými stanicami s operačným systémom Windows. Inštalácia je pomerne jednoduchá, jediným parametrom je názov počítača a pracovnej skupiny. K výhodám patrí dosahovaná prenosová rýchlosť a minimálne nároky na konfigurovateľnosť. Bohužiaľ tento protokol nie je routovateľný (t.j. komunikáciu v sieti nie je možné požadovaním spôsobom smerovať[1]). Preto sa nedá použiť k pripojeniu lokálnej siete do siete Internet. Často sa teda používa súčasne s iným routovateľným protokolom (napr. TCP/IP).

IPX/SPX

Komunikačný protokol IPX/SPX (Internetwork Packet eXchange/Sequenced Packet Exchange) bol vyvinutý pre potreby operačného systému Novell NetWare. V podstate sa nejedná o jeden protokol, ale o skupinu protokolov. Používa sa pri komunikácii medzi

[1] Vyžaduje priame spojenie dvoch bodov v sieti bez medzičlánku

počítačmi s OS Windows a Novell NetWare. Je jednoducho konfigurovateľný. IPX/SPX je routovateľný protokol.

TCP/IP

Komunikačný protokol TCP/IP (Transmission Control Protokol/Internet Protocol) je v súčasnosti **najpopulárnejším komunikačným protokolom**. Nejedná sa o jediný protokol ale o skupinu protokolov .
Dôvodom pre potrebu viacerých protokolov je komplikovanosť problémov, ktoré treba riešiť. Riešenie prebieha na niekoľkých úrovniach a na každej z nich sa používa inú druh protokolov.
Protokol TCP/IP je univerzálny v tom zmysle, že je možné ho používať pri komunikácii **medzi počítačmi s rôznymi OS**. Je routovateľný a vďaka tomu sa stal štandardom pre komunikáciu v sieti Internet.

Model TCP/IP má 4 vrstvy. Zhora nadol sú to vrsty: **aplikačná** (application), **transportná** (transport), **sieťová** (network), a **vrstva sieťového rozhrania** (network interface). Každá vrstva má svoj daný účel.

- **aplikačná vrstva**
  - Zabezpečuje komunikáciu medzi konkrétnymi typmi programov. Napríklad HTTP protokol slúži na komunikáciu medzi prehliadačom webových stránok a webovým serverom, FTP protokol na posielanie súborov, DNS protokol na preklad doménových mien na IP adresy a naopak, SMTP, POP a IMAP protokoly na posielanie mailov a podobne. Do tejto skupiny patrí aj množstvo protokolov na jedno použitie, ktoré si môže navrhnúť pre svoj sieťový program každý programátor.
  - základná jednotka informácie, ktorú si medzi sebou posielajú sieťové programy, je ***správa*** (message)
- **transportná vrstva**
  - Hlavnou úlohou je zabezpečiť spojenie dvoch procesov (spustených programov) na rôznych počítačoch. To umožňuje využívanie viacerých sieťových aplikácií súčasne na jednom počítači. **Keď dorazí k počítaču paket, protokol transportnej vrstvy musí určiť, ktorému procesu poskytne dáta v tomto pakete. Táto vrstva tiež zabezpečuje rozdelenie správ na menšie časti, ktoré sa vojdú do paketov.** Na internete sa najčastejšie používajú z transportných protokolov dva: **TCP** a **UDP**. TCP protokol k hlavnej úlohe ešte pridáva ďalšiu funkcionalitu. Zabezpečuje spoľahlivé doručenie všetkých dát v správnom poradí, rieši kontrolu zahltenia (spomalí odosielanie, ak niektorý uzol na ceste je zahltený) a kontrolu toku dát (odosielanie rýchlosťou, ktorou zvláda prenášať najužšie miesto spojenia).
  - paket z pohľadu tejto vrstvy sa nazýva ***transportný datagram***
- **sieťová vrstva**
  - Úlohou sieťovej vrstvy je dopraviť na základe IP adresy príjemcu paket na ľubovoľné miesto na internete z jednej siete do inej. Na tejto vrstve sa už nerieši, čo sa s paketom na cieľovom zariadení stane. Hlavným problémom tejto vrstvy je nájdenie vhodnej cesty pre paket smerujúci na danú IP adresu. Dôležitú úlohu tu majú smerovacie protokoly.
  - paket z pohľadu tejto vrstvy sa nazýva ***sieťový paket***
- **vrstva sieťového rozhrania**

- Úlohou je dopraviť paket vo vnútri podsiete k správnej sieťovej karte daným fyzickým médiom. Každá sieťová karta má danú svoju MAC adresu.(MAC adresa je spravidla 48-bitové číslo, ktoré sa pre prehľadnosť uvádza ako 12-miestne hexadecimálne číslo (napr. 08:00:69:02:01:FC) Pre prijatie paketu, ktorý "ide okolo počítača", sieťovou kartou je dôležitá MAC adresa. Použitá technológia je závislá na type spoja (optický kábel, kovový drôt, bezdrôtový spoj), na vlastnostiach týchto spojov aj použitej topológii zapojenia. Typické technológie sú Ethernet, Wireless LAN, Bluetooth, Point-to-point, Token ring a iné.
- paket z pohľadu tejto vrstvy sa nazýva ***rámec*** (frame)

Protokoly aplikačnej vrstvy:

DHCP (Dynamic Host Resolution Protocol) – tento protokol sa využíva pre dynamické prideľovanie IP adries (jedinečný identifikátor počítača v sieťach s protokolom TCP/IP). Na niektorom z počítačov v sieti (najčastejšie je to server) je inštalovaná služba DHCP server, ktorá sa stará o dynamické prideľovanie IP adries klientom (miesto ručného nastavovania každej stanice samostatne. Počítače, ktoré sú nastavené ako DHCP klienti nepotrebujú žiadne ďalšie nastavenia. Získajú ich od DHCP servera a tieto nastavenia sú neviditeľné pre bežného používateľa.). Samozrejme IP adresu klientom môžeme prideliť aj staticky (napevno).

DNS (Domain Name Service) – úlohou tejto služby je preklad plného mena domény do číselnej podoby v tvare IP adresy. Keďže pri komunikácii používajú počítače IP adresy a ľudia si skôr zapamätajú doménové meno počítača, bol vytvorený systém DNS na preklad doménového mena na IP adresu, resp. naopak.

SMTP (Simple Mail Transfer Protocol) – poskytuje jednoduchú službu elektronickej pošty. Využíva protokol TCP pre odosielanie a prijímanie správ elektronickej pošty.

FTP (File Transef Protocol) – protokol využívaný na prenos súborov medzi vzdialenými počítačmi. Ak chcem s týmto protokolom pracovať, je nutné aby na počítači ku ktorému sa pripojujeme bola spustená služba FTP server.

HTTP (HyperText Transport Protocol) - protokol určený k prenosu hypertextových dokumentov cez internet. K svojej funkcii vyžaduje server - HTTP server a klienta HTTP (napr. internetový prehliadač).

HTTPS (HyperText Transport Protocol Secure) – variant protokolu HTTP pre bezpečný prenos.

Model ISO/OSI

TCP/IP je označenie viacerých protokolov, ktoré sa používajú pri komunikácií prostredníctvom Internetu. Dôvodom pre potrebu viacerých protokolov je komplikovanosť problémov, ktoré treba riešiť. Riešenie prebieha na niekoľkých úrovniach a na každej z nich sa používa inú druh protokolov. Hovoríme o vrstvách.
Pôvodný model prepojovania otvorených systémov (z pohľadu počítačových sietí sa takto nazýva aj sieť Internet) bol štvorvrstvový. Neskoršie bol prepracovaný, doplnený a v roku 1984 prijatý v súčasnosti používaný sedemvrstvový referenčný model, označovaný ako

OSI (Open System Interconnection). Vypracovala ho medzinárodná štandardizačná organizácia ISO a obsahuje samozrejme aj štyri vrstvy predošlého modelu.
V tomto modeli je najnižšie položená vrstva fyzická, ktorú tvoria hardverové prostriedky (vodiče, sieťové karty atd.) a najvyššie aplikačná vrstva, ktorú tvoria najčastejšie užívateľské programy (napr. Netscape Communicator, Internet Explorer, Word atd.).
Od okamihu, keď užívateľ odošle dáta zo svojej sieťovej aplikácie po ich fyzickú prítomnosť v sieti, prejdú údaje niekoľkými myslenými vrstvami.

1. **aplikačná vrstva (application)** Program
2. **prezentačná vrstva (presentation)** prevod do tvaru zrozumiteľného pre príjemcu
3. **relačná vrstva (session)** vytvorenie a údržba spojenia s príjemcom
4. **transportná vrstva (transport)** dozor na spoľahlivý prenos správ a opravy chýb
5. **sieťová vrstva (network)** Vytvorenie paketu s adresami a ostatnými nutnými časťami
6. **spojová vrstva (data-link)** vytvorenie rámcov a ich vysielanie
7. **fyzická vrstva (physical)** prenos rámcov vo forme elektrických signálov

Vyššia vrstva využíva služby nižšej vrstvy (ako africký a indický biológ).

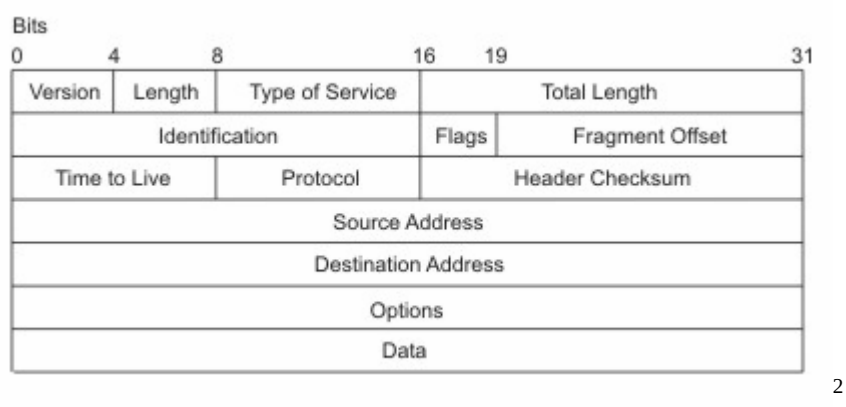
Fyzická vrstva
Fyzická vrstva zabezpečuje prenos informácií vo forme elektrických alebo optických signálov. Pomocou nich prebieha komunikácia medzi počítačmi, preto vlastnosti tejto vrstvy sú vopred starostlivo definované. Dostane od spojovej vrstvy postupnosť núl a jednotek a poesiela ich ďalej. Prepojovacím uzlom na tejto vrstve môže byť **opakovač (repeater)**.

Spojová vrstva
Spojová vrstva zaisťuje v prípade sériových liniek výmenu dát medzi susednými počítačmi a v prípade lokálnych sietí výmenu dát **v rámci lokálnej siete**. Na fyzickej vrstve sa neidentifikuje cieľ, tu už áno. Riadi sa tu aj spôsob prístupu k médiu (nemôžu začať všetci naraz „kričať“ do jedného kábla :-)). Základnou jednotkou pre prenos dát je na linkovej vrstve **dátový rámec**. Dátový rámec sa skladá zo záhlavia (Header), prenášaných dát (Payload) a pätičky (Trailer).
Dátový rámec nesie v záhlaví linkovú adresu príjemcu, linkovú adresu odosielateľa a ďalšie riadiace informácie.
V pätičke nesie okrem iného obvykle kontrolný súčet z prenášaných dát (Pomocou neho je možné zistiť pri prenose chybný prenos (porušenie) dát).
Štandardne vyzerá rámec takto:

8 bajtov	6 bajtov	6 bajtov	2 bajty	46 – 1500 bajtov	4 bajty
preambula	cieľová MAC adresa	zdrojová MAC adresa	typ protokolu vyššej vrstvy	telo rámca	CRC

V prenášaných dátach je potom spravidla nesený paket sieťovej vrstvy.
Prepojovacím uzlom na tejto vrstve môže byť **most (bridge) alebo switch**.

Sieťová vrstva
Sieťová vrstva zabezpečuje prenos dát medzi vzdialenými počítači WAN (smerovanie). Jej úlohou je odoslať data do cieľovej siete. Základnou jednotkou prenosu je **sieťový paket**, ktorý sa balí do dátového rámca. Sieťový paket sa tiež skladá zo záhlavia a dátového poľa. S pätičkou sa u sieťových protokolov stretávame len zriedka.
Štandardne vyzerá takto:



[2]

V rozsiahlych sieťach (WAN) medzi počítačmi leží spravidla jeden alebo viac smerovačov (router). Medzi susednými smerovačmi je na linkovej vrstve vždy priame spojenie. Smerovač vybalí sieťový paket z dátového rámca (jedného linkového protokolu) a pred odoslaním do inej linky ho opäť zabalí do iného dátového rámca (obecne iného linkového protokolu).
Prepojovacím uzlom na tejto vrstve môže byť **smerovač (router).**

Transportná vrstva

Sieťová vrstva zabezpečí spojenie medzi vzdialenými počítačmi, takže transportnej vrstve sa javí akoby žiadne modemy, opakovače, mosty či smerovače na ceste neboli. Transportná vrstva sa celkom spolieha na služby nižších vrstiev. Tiež predpokladá, že spojenie medzi počítačmi je zaistené, preto sa bez zbytočných starostí môže venovať spojeniu medzi aplikáciami na vzdialených počítačoch. (Vôbec tu nevidíme, či sa rozprávame so stanicou vedľa nás, alebo na druhom konci sveta)
Z hľadiska sieťovej vrstvy sú pakety adresované adresou počítača (resp. jeho sieťového rozhrania). Z hľadiska transportnej

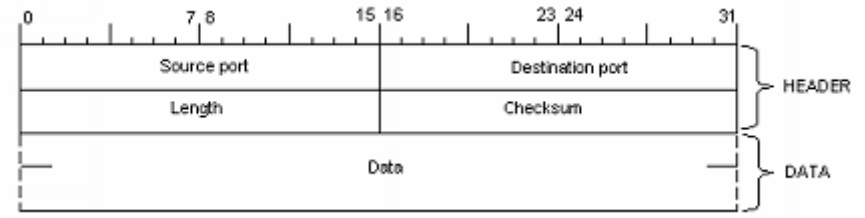
---

[2]

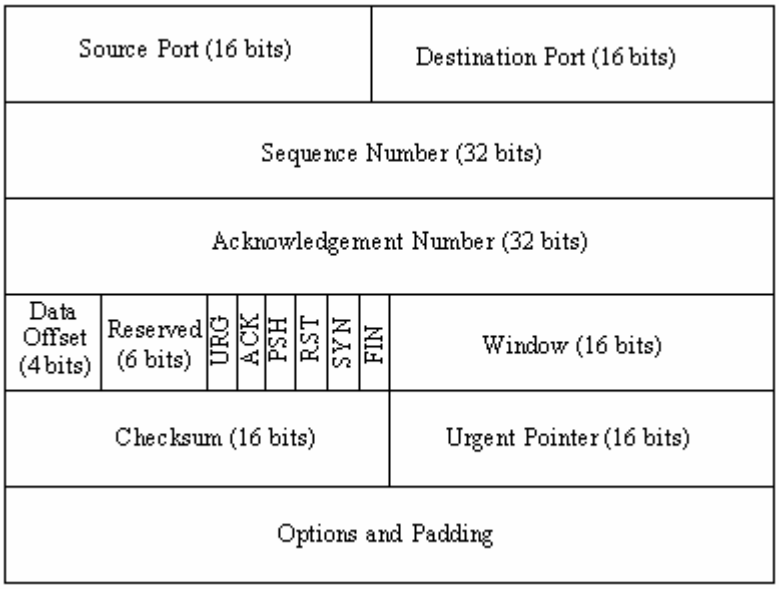
- **version** - *verzia* IP protokolu
- **length** - *dĺžka hlavičky*
- **type of service** - v preklade *typ služby* - Určuje charakter dát prenášaných v tomto IP datagrame. Typ služby tak určuje prioritu datagramu, ktorá sa môže brať do úvahy pri zaraďovaní vo výstupných radoch rozhraní routrov. V type služby sa dá v prípade potreby špecifikovať požiadavka na malé zdržanie, vysokú priepustnosť a/alebo vysokú spoľahlivosť.
- **total length** - *celková dĺžka* - Predstavuje počet bajtov celého IP datagramu. Maximálna dĺžka je závislá od typu siete a je označovaná aj ako **MTU** teda **maximal transfer unit**. V Ethernete sa bežne používa MTU 1500 bajtov.
- **identification** - Určuje jedinečné číslo datagramu. Toto číslo sa používa na to, že ak po ceste dôjde k fragmentácii paketu, každý fragment bude mať toto číslo rovnaké a na základe toho bude prijímajúca strana vedieť, ktoré fragmenty patria k sebe.
- **flags** - *príznaky* - Sú iba dva:
  - **DF** – 0 znamená, že datagram môže byť fragmentovaný a 1 znamená, že nemôže.
  - **MF** – 0 znamená, že ide o posledný z fragmentov pôvodného datagramu a 1 znamená, že to nie je posledný fragment pôvodného datagramu.
- **fragment offset** – Určuje, od ktorej pozície z tela pôvodného datagramu začínajú dáta v tomto fragmente. Pozícia sa určuje v 8 bajtových jednotkách.
- **time to live**, často uvádzaný iba ako skratka *TTL* – Určuje, cez koľko routrov môže datagram na svojej ceste maximálne prejsť. Pri každom prechode routrom sa toto číslo znižuje o 1. Ak na router príde datagram s TTL 1, je datagram automaticky zahodený.
- **protocol** - Toto políčko sa použije, až keď datagram príde do cieľovej stanice. Určuje to, aký protokol je použitý v tele datagramu. Typicky to môže byť identifikácia toho, že v datagrame je prenášaný segment transportného protokolu TCP alebo UDP.
- **header checksum** - *Kontrolný súčet hlavičky* sa robí rovnako ako v prípade protokolov TCP a UDP, sčítavaním 16 bitových úsekov hlavičky.
- **source adddress** - *zdrojová adresa* - 32 bitová adresa zdrojovej stanice.
- **destination adddress** - *cieľová adresa* - 32 bitová adresa cieľovej stanice. Viac o adresácii v IPv4 sieťach je popísané nižšie.
- **options**, alebo *voľby* je nepovinná súčasť hlavičky. Ich použitie často zbytočne znižuje výkon routrov a je snaha ich nepoužívať. Môžu obsahovať rôzne doplňujúce údaje ku bezpečnosti, smerovaniu, identifikáciu prúdov dát alebo časové pečiatky.

vrstvy sú adresované jednotlivé aplikácie (smerovače dopravia na základe IP adresy, tu ešte musíme rozhodnúť, ktorej aplikácii to patrí na základe čísla portu). Aplikácie sú jednoznačné adresované v rámci jedného počítača.
Jednotkou prenosu je **transportný paket (datagram)**, ktorý sa opäť skladá zo záhlavia a dátovej časti. Datagramy môžu byť dvoch typov:

- **bez spojenia (UDP)-** nečakáme na odpoveď
  Protokol neobsahuje žiadnu inicializáciu ani uzatváranie spojenia. To znamená, že nie je potrebné ani uchovávanie stavu spojenia v koncových staniciach. Dáta sú odosielané k cieľu bez toho, aby bolo vyžadované potvrdenie prijatia správ. Dokonca môže ísť iba o jednosmerné vysielanie bez akejkoľvek spätnej reakcie. Typickým príkladom, kde sa to využíva je streamovanie rádia a televízií.
  UDP datagram vyzerá takto:



- **so spojením (TCP)-** čakáme na odpoveď – podobne ako telefón – nadviažeme spojenie, priebežne zisťujeme, či spojenie funguje, nakoniec spojenie ukončíme
  Hlavička TCP datagramu vyzerá takto:



Transportný paket sa prenáša v dátovej časti sieťového paketu.
Pri vysielaní zabezpečuje segmentáciu dlhých správ do paketov a pri príjme zloženie paketov do pôvodnej správy.

Relačná vrstva
Relačná vrstva zabezpečuje výmenu dát medzi aplikáciami, tj. prevádza tzv. checkpoint (kontrolné body – ak napríklad niečo sťahujem a preruší sa spojenie, tak keď sa spojenie obnoví, pokračujem v sťahovaní v tom bode, kde som skončil), synchronizáciu transakcií (rieši problém súvisiaci so súťažením procesov o zdroje), korektné uzatváranie súborov, obnovenie relácie v prípade výpadku spojenia…

Dobre predstaviteľnou reláciou je napr. zdieľanie sieťového disku. Disk môže byt zdieľaný po určitú dobu, avšak pracuje sa s ním len zriedka. Vždy, keď je napr. treba pracovať so súborom na sieťovom disku, nadviaže sa na dobu od otvorenia súboru až po jeho uzavretie spojenie na transportnej vrstve. Avšak relácia na relačnej vrstve existuje po celú dobu zdieľania disku. Nadväzuje, udržiava a ruší logické spojenia - relácie medzi koncovými účastníkmi. Základnou jednotkou je relačný paket, ktorý sa opäť vkladá do transportného paketu.

Prezentačná vrstva
Prezentačná vrstva je zodpovedná za reprezentáciu a zabezpečenie dát.
Reprezentácia dát môže byt na rôznych počítačoch rôzna (napr. rôzne počítače si môžu ukladať čísla rôzne – teda v pamäti to vyzerá rôzne). Táto vrstva sa stará aby sa tieto rozdiely zakryli.
Zabezpečením sa rozumie šifrovanie, zabezpečenie integrity dát (tzn. záruku, že dáta boli prijaté/prečítané bez chýb), digitálne podpisovanie a pod.

Aplikačná vrstva
Aplikačná vrstva predpisuje v akom formáte a ako majú byt dáta preberané/predávané od aplikačných programov. Teda na tejto vrstve nás budú zaujímať protokoly…

Použitá literatúra:

- Kostrhoun, A.: Stavíme si malou síť. Praha: Computer Press, 2001. ISBN 80-7226-510-5
- Hlavenka, J.: Výkladový slovník výpočetní techniky a komunikací. Praha: Computer Press, 1997. ISBN 80-7226-023-5
- Cisco Systems, Inc. IP Addressing and Subnetting for New Users. [online] Publikované 26. 12. 2003. Dostupné z <http://www.cisco.com/warp/public/701/3.html>.
- HALČIN Pavol. Počítačové siete. [online] Publikované 18.2.2002. Dostupné z <http://www.gymsnv.sk/~x8ahalp/net_web/>.
- Počítačové siete [online] Dostupné z <http://www.spsmt.sk/phare/>.
- České IPv6. [online] Dostupné z <http://www.ipv6.cz >.

Gursky: prednášky zo sietí <http:// ics.upjs.sk/~gursky/siete>
Jirásek: prednášky zo sietí