Networking

Portál:	edu.ukf.sk - Vzdelávací portál - Univerzita Konštantína Filozofa, Nitra
Kurz:	Operačné systémy (KI/OS/15)
Kniha:	Networking
Vytlačil(a):	Zuzana Pavlendová
Dátum:	Streda, 1 december 2021, 17:59

Opis

7 NETWORKING

7.1 Sieťový model a sieťová architektúra

7.1.1 Fyzická vrstva

7.1.2 Linková (spojová) vrstva

7.1.3 Sieťová vrstva

7.1.4 Transportná vrstva

7.1.5 Relačná vrstva

7.1.6 Prezentačná vrstva

7.1.7 Aplikačná vrstva

7.2 Sieťové protokoly

7.2.1 Protokoly NetBIOS a NetBEUI

7.2.2 Protokol IPX/SPX

7.2.3 Protokol TCP/IP

7.2.4 Porovnanie TCP/IP a referenčného modelu ISO/OSI

Obsah

Úvod

V tejto kapitole sa dozviete:

• Prečo sa v modeloch počítačových sietí používa rozdelenie komunikujúcich systémov do vrstiev.

• Ako vznikol referenčný sieťový model ISO/OSI a aké má vlastnosti.

• A ké sú najdôležitejšie sieťové protokoly, resp. protokolové sady používané v počítačových sietiach.

• A ké sú hlavné odlišnosti medzi prakticky používanými protokolovými sadami a referenčným modelom OSI.

Po jeho preštudovaní by ste mali byť schopní:

• Rozumieť štruktúre vrstvových modelov počítačových sietí a spôsobu komunikácie, ktorá v nich prebieha.

• Charakterizovať jednotlivé vrstvy referenčného sieťového modelu ISO/OSI a im vymedzené funkcie.

• Charakterizovať základné vlastnosti protokolových sád NetBIOS/NetBEUI, SPX/IPX, TCP/IP.

• Š pecifikovať základné rozdiely medzi referenčným modelom OSI/OSI a sieťovou architektúrou TCP/IP.

Kľúčové slová tejto kapitoly:

Sieťový model, sieťová architektúra, model vrstvový, model referenčný ISO/OSI, vrstva fyzická, vrstva linková, vrstva sieťová, vrstva transportná, vrstva relačná, vrstva prezentačná, vrstva aplikačná, protokolová sada, NetBIOS/NetBEUI, SPX/IPX, TCP/IP.

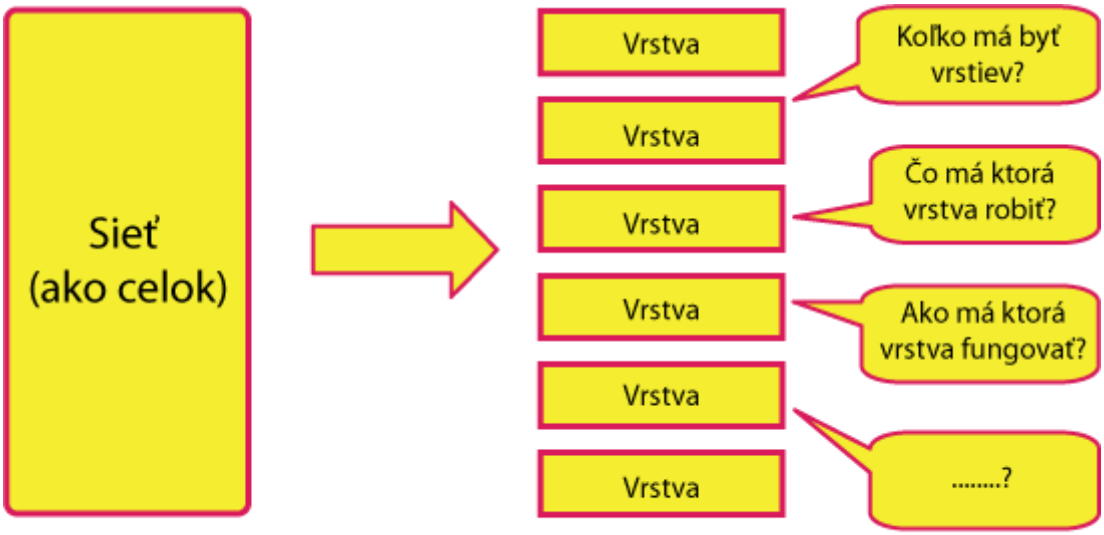
Doba potrebná k štúdiu: 6 hodín

Sp rievodca štúdiom

Cieľom tejto kapitoly je zoznámiť študentov so zásadnými pojmami z oblasti počítačových sietí, pojmu sieťový model a s ním súvisiacich pojmov. Za najpodstatnejšie v tejto kapitole považujeme pochopenie rozdelenia funkcií obecnej počítačovej siete medzi jednotlivé vrstvy referenčného modelu ISO/OSI. Cieľom tejto kapitoly je tiež zoznámiť študentov s najdôležitejšími protokolmi prakticky používanými v počítačových sietiach. Štúdium tejto kapitoly je pomerne náročné predovšetkým z dôvodu zavedenia mnohých nových pojmov, predovšetkým dbajte na správne pochopenie princípov protokolovej sady TCP/IP. Pre štúdium tejto kapitoly si v záujme toho, aby ste mohli dôkladne premyslieť a pochopiť rozdelenie funkcií sietí do jednotlivých vrstiev modelu ISO/OSI, vyhraďte dostatok času.

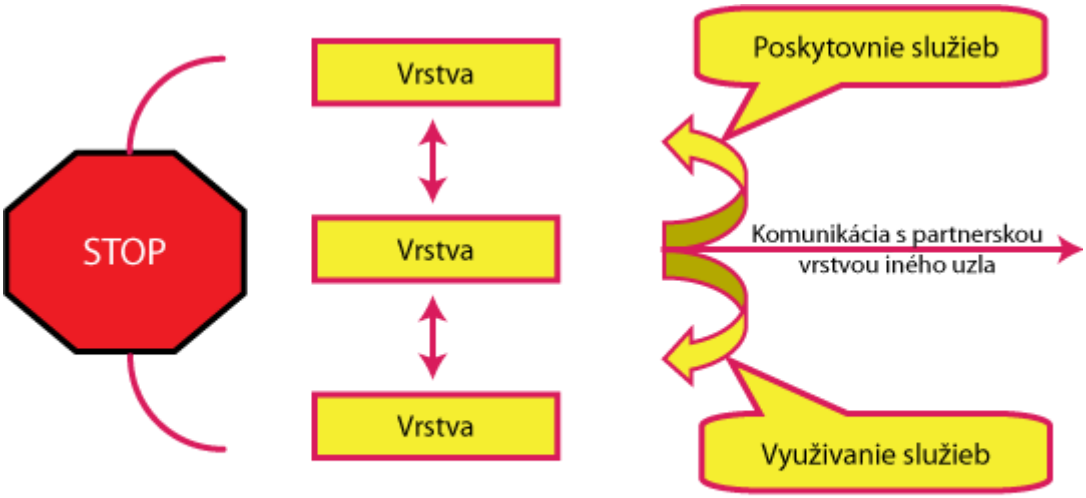
7.1 Sieťový model a sieťová architektúra

Implementovať funkčnú sieť je veľmi zložité a náročné, jedná sa o podobnú situáciu ako pri riešení veľkých SW celkov. Ide o jeden veľký problém, ktorý sa oplatí dekomponovať, to znamená rozdeliť na menšie časti, ktoré je možné riešiť samostatne. Dekompozícia sa vykoná po hierarchicky usporiadaných vrstvách, čo dobre zodpovedá povahe riešeného problému. Prináša to i ďalšie výhody ako aj možnosť alternatívnych riešení na úrovni nižších vrstiev, väčšiu modulárnosť. Predstava dekompozície je zrejmá z nasledujúceho obrázku.

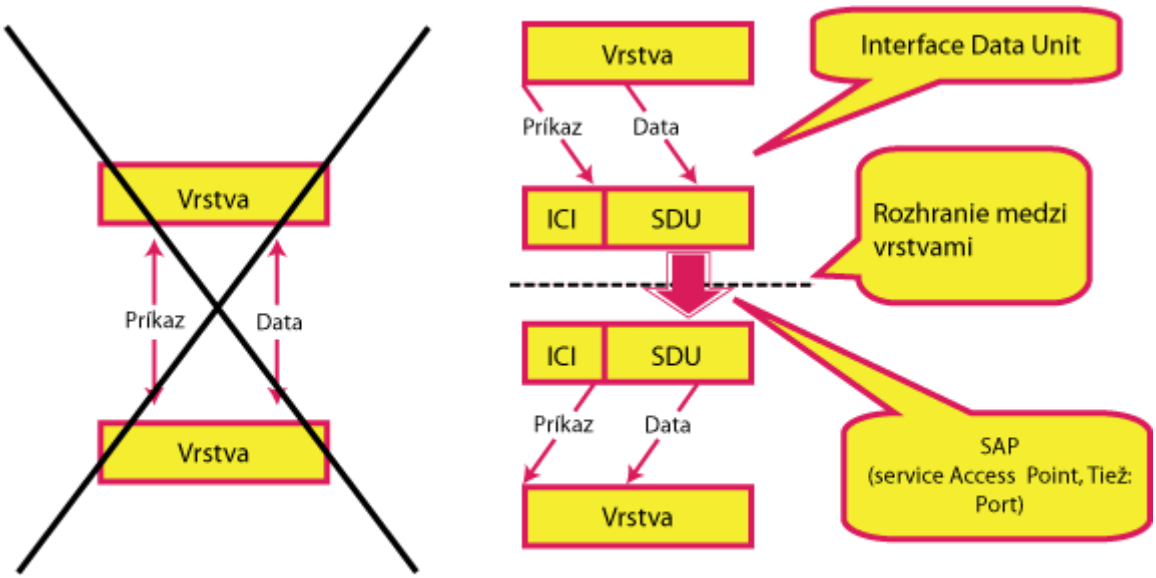


Dekompozícia siete na vrstvy

Spôsob komunikácie medzi vrstvami je zrejmý z nasledujúcich obrázkov.

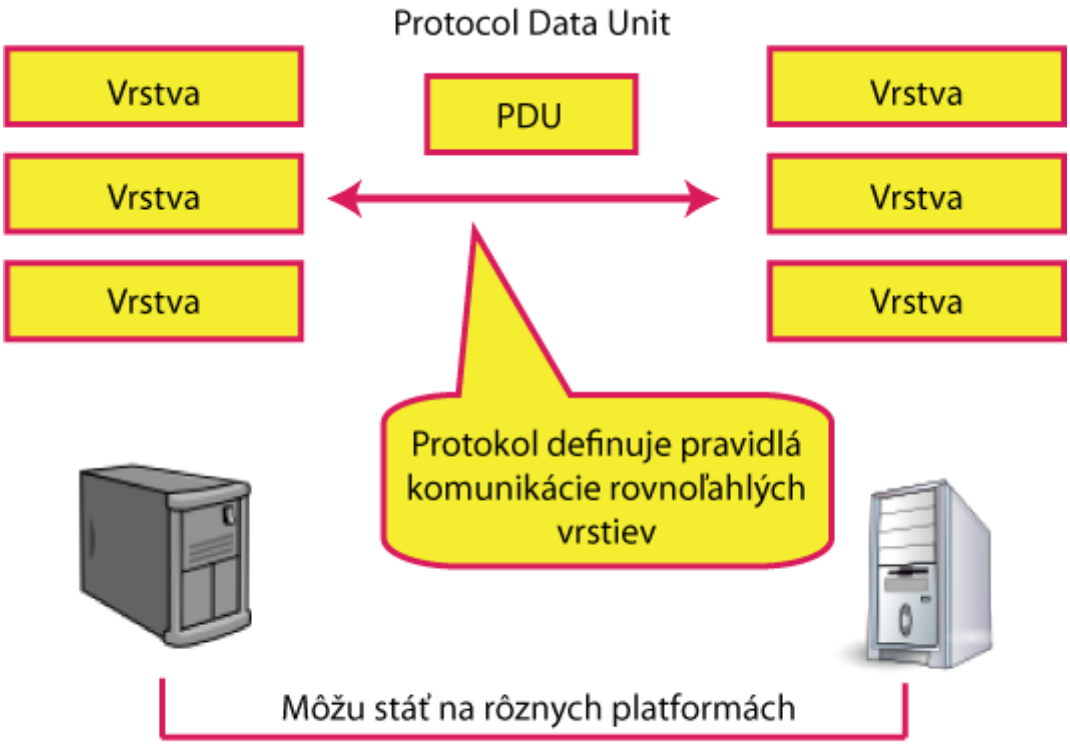


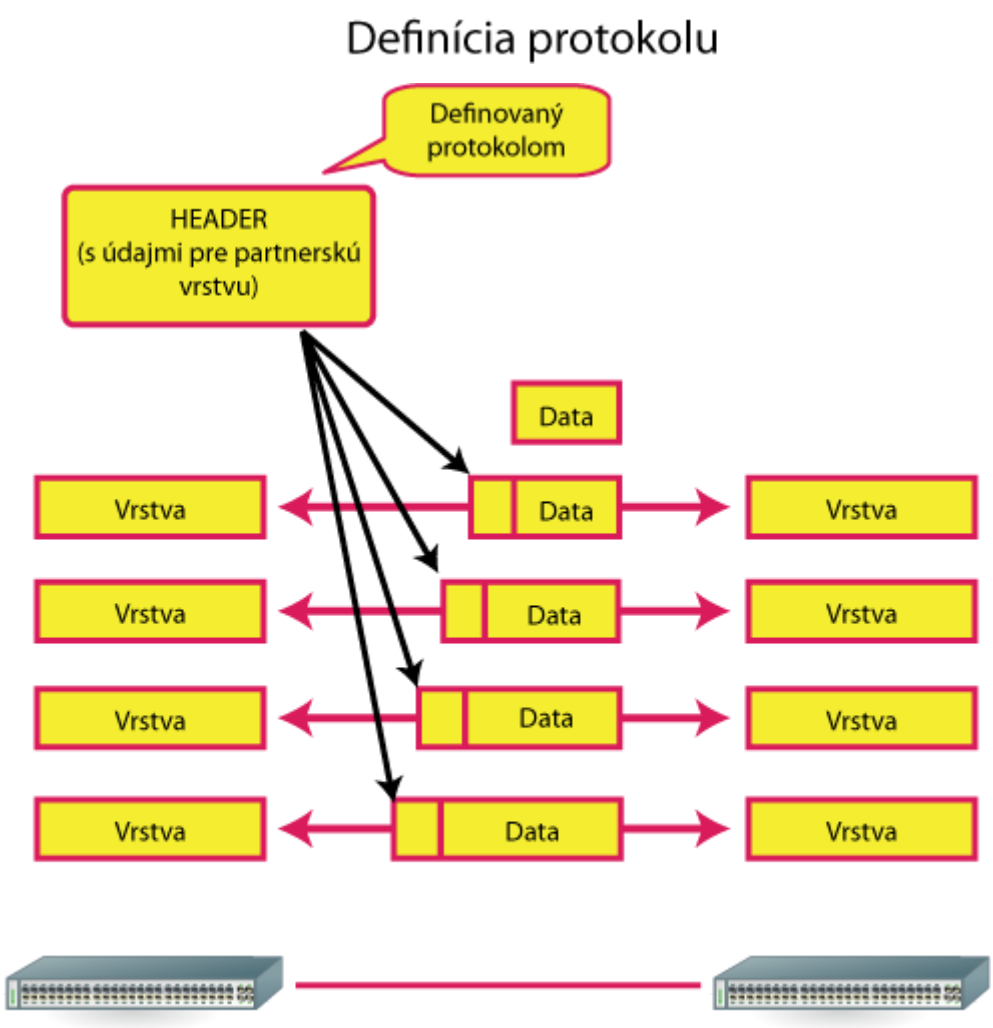
Komunikácia medzi susednými vrstvami



Definícia protokolu

V tejto súvislosti je potrebné vysvetliť pojem protokol. Protokol definuje pravidlá komunikácie na rovnoľahlých vrstvách, pričom komunikujúce subjekty môžu pracovať na rôznych platformách.





Protokoly na jednotlivých vrstvách

Z uvedených obrázkov vyplýva, že vrstvy nie sú „jednoliate“, v každej vrstve môže existovať a fungovať niekoľko relatívne samostatných entít. Pod pojmom entita môžeme chápať napr. proces, démon, úlohu apod. Entity v rovnakej vrstve môžu plniť rozdielne funkcie (nekonkurovať si) alebo plniť podobné funkcie (ale iným spôsobom, konkurovať si). Protokol definuje pravidlá komunikácie medzi entitami rovnoľahlých vrstiev. Každý protokol vždy „patrí“ do určitej konkrétnej vrstvy a určuje spôsob, akým je realizovaná určitá služba. Pre každú vrstvu môže

existovať niekoľko alternatívnych protokolov, pričom súčasné použitie rôznych protokolov (v rámci tej istej vrstvy) sa nemusí vylučovať. Sieťový model je ucelená predstava o tom, ako majú byť siete riešené. Zahŕňa predstavu o počte vrstiev a predstavu o tom, čo má mať ktorá vrstva na starosti.

Nezahŕňa konkrétnu predstavu o tom, ako má ktorá vrstva svoje úkoly plniť. Sieťová architektúra obsahuje naviac tiež konkrétnu predstavu o spôsobe fungovania jednotlivých vrstiev, tj. obsahuje i konkrétne protokoly. Príkladom sieťového modelu je referenčný model ISO/OSI a príkladom sieťovej architektúry je TCP/IP. V niekoľkých uplynulých rokoch bol vyvinutý rad sieťových noriem. Niektoré rozhodujúce organizácie v tomto obore vytvorili protokoly alebo pravidlá, ktoré zaisťujú kompatibitu pre sieťový hardvér a softvér rôznych výrobcov. Dosiaľ sme si všímali hlavné komponenty sietí LAN. Keby boli počítače, aplikačné programy, sieťový softvér a kabeláž vyrobené rovnakým dodávateľom, nebol by žiadny problém zaistiť, aby všetko hladko spolupracovalo. Dnešná realita je však taká, že obvykle sieťový softvér jedného výrobcu LAN nebude pracovať v sieti jeho konkurenta, takže aplikačné programy a dokonca i kabeláž musí byť vybraná pre určitú sieť LAN. Aby bola dosiahnutá aspoň nejaká úroveň zjednotenia medzi rôznymi dodávateľmi sietí, vytvorila organizácia ISO normy nazvané OSI (Open Systems Interconnection). Rôzne počítače vzájomne prepojené do siete musia vedieť, v akej forme budú prijímať informácie. Kde je začiatok určitého slova, kde je jeho koniec a kde začne slovo nasledujúce? Má počítač možnosť zistiť, či bola správa pri prenose skreslená? Model OSI zodpovedá na tieto a ďalšie otázky pomocou radu noriem, ktoré by mali v budúcnosti umožniť verejnosti, aby si kupovala sieťové prvky rôznych dodávateľov s určitou istotou, že budú spolupracovať. Referenčný model ISO/OSI bol pokusom vytvoriť univerzálnu sieťovú architektúru. Skončil ako sieťový model bez protokolov, tie sa dorábali postupne. Pochádza „zo sveta spojov“ od organizáce ISO (International Standards Organization, správne: International Organization for Standardization) - členmi ISO sú národné normalizačné inštitúcie. Bol oficiálnym riešením, dnes je prakticky odpísaný, prehral v súboji s TCP/IP. Referenčný model ISO/OSI reagoval na vznik proprietárnych a uzatvorených sietí IBM SNA. Prvotným zámerom bolo definovať, ako majú vyzerať otvorené systémy. Odtiaľ je názov Open Systems Architecture. Chovanie „vo vnútri“, nielen „medzi sebou“ ukázalo sa ako príliš náročné, došlo k redukcii ambícií. Preto nastalo druhé priblíženie, ktoré sa týkalo len vzájomného prepojenia otvorených systémov a nastala zmena názvu na Open Systems Interconnection Architecture. Opäť sa ukázalo ako príliš náročné a preto nastalo tretie priblíženie, ktoré neobsahovalo konkrétne protokoly, ale len predstavu o počte vrstiev a o tom, čo má ktorá vrstva robiť. Posledná iterácia názvu je teda Open Systems Interconnection. Boli odstránené protokoly, zostal len sieťový model, teda obecný „rámec“, do ktorého sú konkrétne riešenia „zasadzované“ a konkrétne protokoly pre RM ISO/OSI sú vyvíjané samostatne a najprv dodatočne sú zaraďované do rámca ISO/OSI. Filozofia RM ISO/OSI vznikala „od zeleného stola“ a potom bol „nadiktovaný“ používateľom. Vznikala maximalistickým spôsobom a autori sa snažili zahrnúť „všetko, čo by sa niekedy niekomu mohlo hodiť“. Výsledok bol dosť odtiahnutý od reálnej praxe, celé riešenie sa často ukázalo ako nerealizovateľné, a hľadala sa implementovateľná podmnožina, avšak vzájomne kompatibilná. Mnohé východiskové predpoklady sa ukázali ako chybné. Autori ISO/OSI sa dosť dlho dohadovali o počte vrstiev, nakoniec zvíťazil návrh na 7 vrstiev a dnes sa to zdá byť zbytočne veľa. Kritériá pre voľbu vrstiev boli stanovené nasledovne:

• činnosti na rovnakom stupni abstrakcie majú patriť do rovnakej vrstvy,

• odlišné funkcie by mali patriť do odlišných vrstiev,

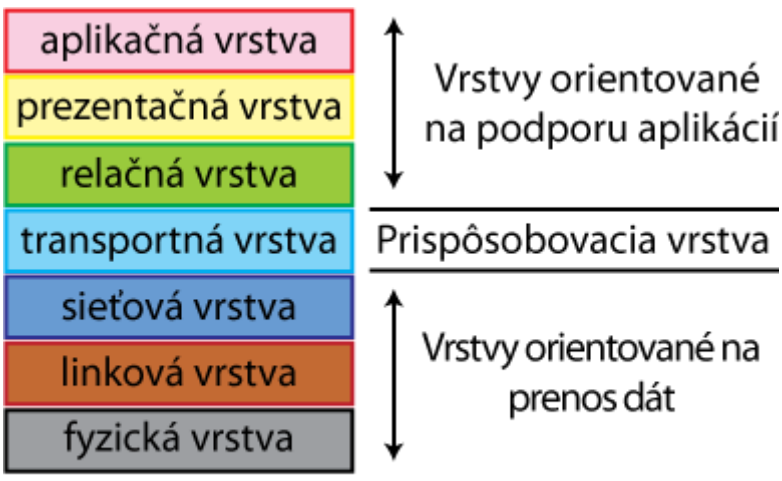
• aby bolo možné prevziať už existujúce štandardy,

• aby datové toky medzi vrstvami boli čo najmenšie,

• aby vrstvy boli rovnomerne vyťažené.

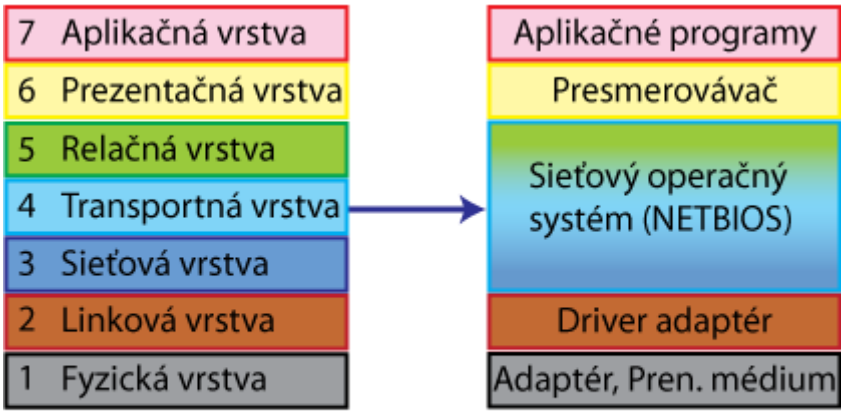
Štandard OSI (Open Systems Interconnection) predstavuje model so siedmimi vrstvami, ktorý zaisťuje účinnú komunikáciu v rámci siete LAN a tiež medzi rôznymi sieťami. Model OSI sa skladá zo siedmych vrstiev špecifikácií, ktoré popisujú manipuláciu s dátami pri jednotlivých fázach prenosu. Každá vrstva poskytuje určité služby vrstve, ak je bezprostredne nad ňou. Sedem vrstiev ISO/OSI je na nasledujúcom obrázku

Orientácia vrstiev je zrejmá z nasledujúceho obrázka.



Orientácia vrstiev ISO/OSI

Každá vrstva vykonáva vlastné služby pričom zaisťuje náväznosť na susedné vrstvy.



Vrstvy modelu ISO/OSI

Model OSI priraďuje zložitým procedúram, nevyhnutným pre komunikáciu v sieti, sedem rôznych vrstiev. Model je navrhnutý tak, aby bolo možné ľahko dosiahnuť východzajúcej dohody na nižších vrstvách a konečne na všetkých siedmych vrstvách.

7.1.1 Fyzická vrstva

Štandardy fyzickej vrstvy sa týkajú technických noriem zaisťujúcich kompatibilitu sietí. Zahŕňajú použité napäťové úrovne, časovanie prenosu dát a mechanizmy vzájomného potvrdzovania. Prvá vrstva (fyzická) predstavuje rad pravidiel týkajúcich sa technického vybavenia použitého pre prenos dát. Zaoberá sa takými vecami, ako sú napäťovej úrovne, časovanie prenosu dát a pravidlá pre komunikáciu, ktorá slúži k vytvoreniu spojenia. Fyzická vrstva určuje, či majú byť bity odosielané v poloduplexnom režime (to je podobné spôsobom, akými sa dáta odovzdávajú pomocou rádiostanice) alebo v plne duplexnom režime, čo vyžaduje súčasné vysielanie i príjem dát. Ďalšia technická špecifikácia, ktorú pokrýva fyzická vrstva, zahŕňa konektory a rozhranie na prenosové médiá.

Na tejto úrovni sa model OSI zaoberá elektrickými veličinami a bitmi (nulami a jednotkami). Bity nemajú na tejto úrovni žiadny skutočný význam. Priradenie významu vykonáva až ďalšia vrstva OSI. Fyzická vrstva sa zaoberá výhradne prenosom bitov (bez ohľadu na ich význam), otázkami typu kódovania, modulácie, časovania, synchronizáciou, elektrickými parametrami signálov, konektormi, riadiacimi signálmi rozhrania. Ponúka služby typu prijmi bit a odošli bit a musí zaistiť, že v prípade vysielania jednotkového bitu ho druhá strana prijme ako jednotkový a nie ako nulový. Nijak neinterpretuje to, čo prenáša a jednotlivých bitom neprisudzuje žiadny špecifický význam. Na úrovni fyzickej vrstvy rozlišujeme paralelný a sériový prenos, synchrónny, asynchrónny a arytmický prenos, prenos v základnom a preloženom pásme. Štandardom fyzickej vrstvy je RS-232-C, V.24, X.21. 45

7.1.2 Linková (spojová) vrstva

Spojová vrstva sa zaoberá zhlukovaním dát do rámcov (frame), v ktorých sú prenášané. Model OSI je navrhnutý tak, že každá vrstva poskytuje vyššej vrstve určitý kľúčový prvok. Fyzická vrstva odovzdáva spojovej vrstve bity. A teraz prichádza okamih, kedy je týmto bitom potrebné dať nejaký význam. V tomto bode sa už nezaoberáme bitmi, najskôr dátovými rámcami (pakety), obsahujúcimi ako dáta, tak riadiace informácie. Spojová vrstva pridáva na začiatok a na koniec správy značky (flag). Normy tejto vrstvy vykonávajú dve dôležité funkcie. Zaručujú, že dáta nie sú zamenené za značky a preverujú výskyt chýb vo vnútri dátového rámca.

Toto preverovanie chýb môže prebiehať tak, že sa na stranu prijímača odošle informácia o určitom dátovom rámci a potom sa čaká na potvrdenie, že všetko bolo správne prijaté. Linková vrstva (spojová vrstva) prenáša celé bloky dát tzv. rámce (frames) a zaisťuje prenos iba v dosahu priameho spojenia bez „prestupných staníc“. Môže fungovať spoľahlivo či nespoľahlivo, spojovane či nespojovane a môže využívať rôzne prenosové technológie - linkové i bezdrôtové. Úlohou je synchronizácia na úrovni rámcov (správne rozpoznanie začiatku a konca rámca, i všetkých jeho častí), zaistenie spoľahlivosti (detekcia chýb a náprava), riadenie toku (aby vysielajúci nezahltil príjemcu) a prístup k zdieľanému médiu (rieši konflikty pri viacnásobnom prístupe k zdieľanému médiu). Linková vrstva riadi prístup používateľa na sieť a tvorí obálku paketov. Úlohou je zmeniť jednoduché komunikačné vybavenie na spoj, ktorý sa voči sieťovej vrstve chová ako bezchybný.

7.1.3 Sieťová vrstva

Sieťová vrstva sa zaoberá prepojovaním paketov. Vytvára virtuálne spojenie pre dátovú komunikáciu medzi počítačmi alebo teminálmi. Tretia vrstva modelu OSI, sieťová vrstva, sa zaoberá prepojovaním paketov. Vytvára virtuálne spojenie (trasu medzi počítačmi alebo terminálmi) pre dátovú komunikáciu. U odosielateľa sformuje sieťová vrstva správu z transportnej vrstvy do dátových paketov, ktoré potom môžu nižšie dve vrstvy prenášať. Na strane prijímača zreštauruje sieťová vrstva pôvodnú správu. Aby sme pochopili použitie dátových paketov, bude nevyhnutné pozrieť sa na priemyslový štandard, zahŕňajúci spodné tri vrstvy modelu OSI. Je to štandard X.25. Sieťová vrstva prenáša bloky dát označované ako pakety (packets) a zaisťuje doručenie paketov až ku konečnému adresátovi. V prostredí, kde nie je priame spojenie hľadá vhodnú cestu až k cieľu, zaisťuje tzv. smerovanie (routing). Musí si uvedomovať skutočnú topológiu celej siete (obecne), pričom používa rôzne algoritmy smerovania ako adaptívne či neadaptívne, izolované či distribuované. Je poslednou vrstvou, ktorú musí mať prenosová infraštruktúra.

Hlavnou úlohou sieťovej vrstvy je určenie smerovania dát (paketov) v sieti zo zdroja do cieľa a musí riešiť problematiku zahltenia siete, ku ktorej môže dôjsť pri veľkom množstve paketov. Býva v nej zabudovaná tiež účtovacia funkcia ACOUNT k zaisteniu, koľko ktorý používateľ vyslal bitov.

7.1.4 Transportná vrstva

Prvotnou úlohou transportnej vrstvy je rozpoznanie chýb a zotavenie po chybe, zaoberá sa však tiež multiplexom správ a reguláciou toku informácií. Transportná vrstva modelu OSI má mnoho funkcií včítane niekoľkých úrovní na rozpoznávánie chýb a zotavenie po chybe. Na najvyššej úrovni môže transportná vrstva rozpoznávať (či dokonca opravovať) chyby, odhalovať pakety, ktoré boli odoslané v nesprávnom poradí a prirovnávať ich do poradia správneho. Táto vrstva tiež multiplexuje niekoľko správ do jedného spoja a vytvára hlavičky určujúce ktorému spoju ktorá správa patrí. Transportná vrstva tiež reguluje tok informácie tým, že riadi pohyb správ. Transportná vrstva zaisťuje komunikáciu medzi koncovými účastníkmi (end-to-end komunikáciu), pričom môže meniť nespoľahlivý charakter prenosu na spoľahlivý, menej spoľahlivý prenos na viac spoľahlivý, nespojovaný prenos na spojovaný. Pritom vychádza zo skutočnosti, že sa nedá „hýbať" s vlastnosťami a funkciami nižších vrstiev. Vzhľadom k tomu, že vyššie vrstvy môžu chcieť niečo iného, než čo ponúkajú nižšie vrstvy, je úlohou transportnej vrstvy zaistiť potrebné prispôsobenie. Transportná vrstva rozkladá dáta na menšie časti tzv. pakety, rieši problematiku komunikácie koncových používateľov (end-to-end), pričom využíva ku komunikácii záhlavie a riadiacu správu (transportné záhlavie).

7.1.5 Relačná vrstva

Relačná vrstva sa venuje riadeniu siete. Ovláda rozpoznávanie hesiel, procedúry pri hlásení a odhlásení a rovnako dohliada nad sieťou a nad vytváraním prehľadových správ. Dosiaľ sme videli, že model OSI sa zaoberá iba bitmi a dátovými správami a nerozlišuje jednotlivých používateľov v sieti. Relačnú vrstvu si môžeme predstaviť ako vrstvu, ktorej úlohou je riadenie siete. Je schopná prerušiť určitú reláciu a vedie riadne ukončenie relácií. Používateľ komunikuje priamo s touto vrstvou. Relačná vrstva môže preverovať heslo zadané používateľom a umožniť používateľovi, aby prepol z poloduplexného prenosu na plne duplexný. Dokáže určiť, kto hovorí, ako často a ako dlho. Riadi prenosy dát a zodpovedá rovnako za zotavenie systému po jeho výpadku. Konečne relačná vrstva môže sledovať využitie systému a účtovať používateľom spotrebovaný čas. Relačná vrstva zaisťuje vedenie relácií. Relácia môže zaisťovať synchronizáciu, šifrovanie a podporu transakcií. Relačná vrstva kontroluje prístup používateľa

a jeho programov na sieť, dovoľuje spojenie používateľov na rôznych typoch zariadenia, ktorí majú medzi sebou zavedené tzv. relácie (session) a dovoľuje, aby sa používateľ mohol prihlásiť vo vzdialenom viacpoužívateľskom systéme a preniesol súbor medzi dvoma počítačmi. Rieši riadenie dialógu medzi jednotlivými počítačmi.

7.1.6 Prezentačná vrstva

Bezpečnosť siete, prenosy súborov a formátovacie funkcie, sú úlohy prezentačnej vrstvy. Prezentačná vrstva modelu OSI sa venuje bezpečnosti siete, prenosu súborov a formátovacím funkciám. Na bitovej úrovni je prezentačná vrstva schopná kódovať dáta v rade rôznych formátov v ASCII a EBCDIC. Americký štandardný kód pre výmenu informácií (ASCll) je kód pre prenos dát používajúci 7 bitov pre kódovanie znaku a ôsmy bit ako paritný. Je to kód používaný najobecnejšie. Mnoho väčších počítačov IBM používa rozšírené dvojkovo kódovaný desiatkový kód (EBCDIC - Extended Binary Coded Decimal Intechange Code).

Prezentačná vrstva musí byť schopná použiť pre prenos dát ľubovoľný z týchto štandardov. Prezentačná vrstva má na starosti potrebné konverzie z rôznych kódovaní znakov (ASCII, EBCDIC,...), formát čísel, formát štruktúr, polí a ukazovateľov (pointerov). Nižšie vrstvy sa snažia doručiť každý bit presne tak, ako bol odoslaný a pritom rovnaká postupnosť bitov môže mať pre príjemcu iný význam než pre odosielateľa. Prezentačná vrstva určuje tvar dát v akom sú dostupné používateľovi a presmerováva požiadavky používateľa na sieť, vykonáva kódovanie jednotlivých informácií v paketoch - kryptografie z hľadiska utajenia pred nepovolanými používateľmi (ASCII, EBDIC) a spôsob kompresie a zhustenia informácií pre zmenšenie počtu prenášaných bitov. Pre dosiahnutie komunikácie musí prezentačná vrstva v oboch vzájomne komunikujúcich počítačoch obsahovať tie isté protokoly alebo pravidlá pre manipuláciu s dátami.

Táto vrstva vykonáva rovnako konverziu protokolov medzi rôznymi počítačmi používajúcimi rôzne formáty. Väčšina funkcií textových procesorov, ktoré spájame s formátováním textu (stránkovanie, počet liniek na obrazovke, pohyby kurzoru po obrazovke) je rovnako náplňou prezentačnej vrstvy. Práca s terminálmi, ktoré majú nekompatibilné kódy, je rovnako zaisťovaná touto vrstvou. Terminálový protokol rieši odlišnosti tak, že umožní každému dátovému terminálu aby fungoval ako rovnaký virtuálny terminál. Výsledkom tohto postupu je, že existuje rada prekladových tabuliek fungujúcich medzi miestnym a vzdialeným terminálom. Lokálny terminál vysiela dátovú štruktúru, ktorá definuje okamžitý obsah jeho obrazovky v takých termínoch, ako je zobrazený počet znakov na disku. Tento počet sa môže podstatne líšiť. Mnoho terminálov zobrazuje 132 znakov na riadok, ale existujú i iné formáty. Táto dátová štruktúra prichádza do riadiaceho prvku vzdialeného terminálu a ten prevedie tento počet na taký kód, ktorému terminál rozumie a môže ho použiť. Ďalšie kódy sa používajú pre tučné písmo, podtrhnutie, grafiku atď.

7.1.7 Aplikačná vrstva

Sieťové programy nachádzajúce sa v aplikačnej vrstve zahŕňajú elektronickú poštu, riadenie databází, softvér pre file servery a print servery. Aplikačná vrstva spracováva hlásenie, vzdialené prihlasovanie a zodpovedá za štatistiku riadenia siete. Na tejto úrovni nájdete programy pre riadenie databáz, elektronickú poštu, programy pre file servery a print servery a príkazy operačného systému. Vo väčšine prípadov sú funkcie vykonávané touto vrstvou závislé na používateľovi. Vzhľadom k tomu, že rôzne používateľské programy majú rôzne požiadavky, je obtiažne zovšeobecňovať protokoly, ktoré sa tu nachádzajú. Niektoré odvetvia, napr. bankovníctvo, vyvinulo na tejto úrovni rad vlastných štandardov.

Aplikačná vrstva pôvodne mala obsahovať aplikácie. Problémom je ale veľké množstvo aplikácií a tie by museli byť všetky štandardizované, čo by nemalo ani zmysel. Neskôr bolo definované iba „jadro“ aplikácií, ktoré má zmysel štandardizovať, napríklad prenosové mechanizmy elektronickej pošty a ostatných častí aplikácií (typicky užívateľské rozhranie) boli vysunuté nad aplikačnou vrstvu. Aplikačná vrstva predstavuje vlastne úroveň aplikačných programov napr. elektronická pošta, sieťové databázové systémy, vytvára všeobecne platné protokoly pre prenos dát medzi nekompatibilnými terminálmi, definuje pohyby kurzora po obrazovke, s možnosťou vytvorenia virtuálneho terminálu.

7.2 Sieťové protokoly

Bloky dát predávané medzi koncovými účastníkmi obvykle označujeme ako **pakety** . V ich formátoch nájdeme sieťové adresy oboch koncových účastníkov a informácie potrebné pre potvrdzovanie a prípadne i riadenie toku. Pakety môžu byť predávané ako celkom nezávislé datagramy, alebo ako súčasť súvislejšej komunikácie po virtuálnom kanále. Medzi najdôležitejšie a najpoužívanejšie sieťové protokoly v lokálnych sietiach patrí : NetBEUI, IPX/SPX, TCP/IP.

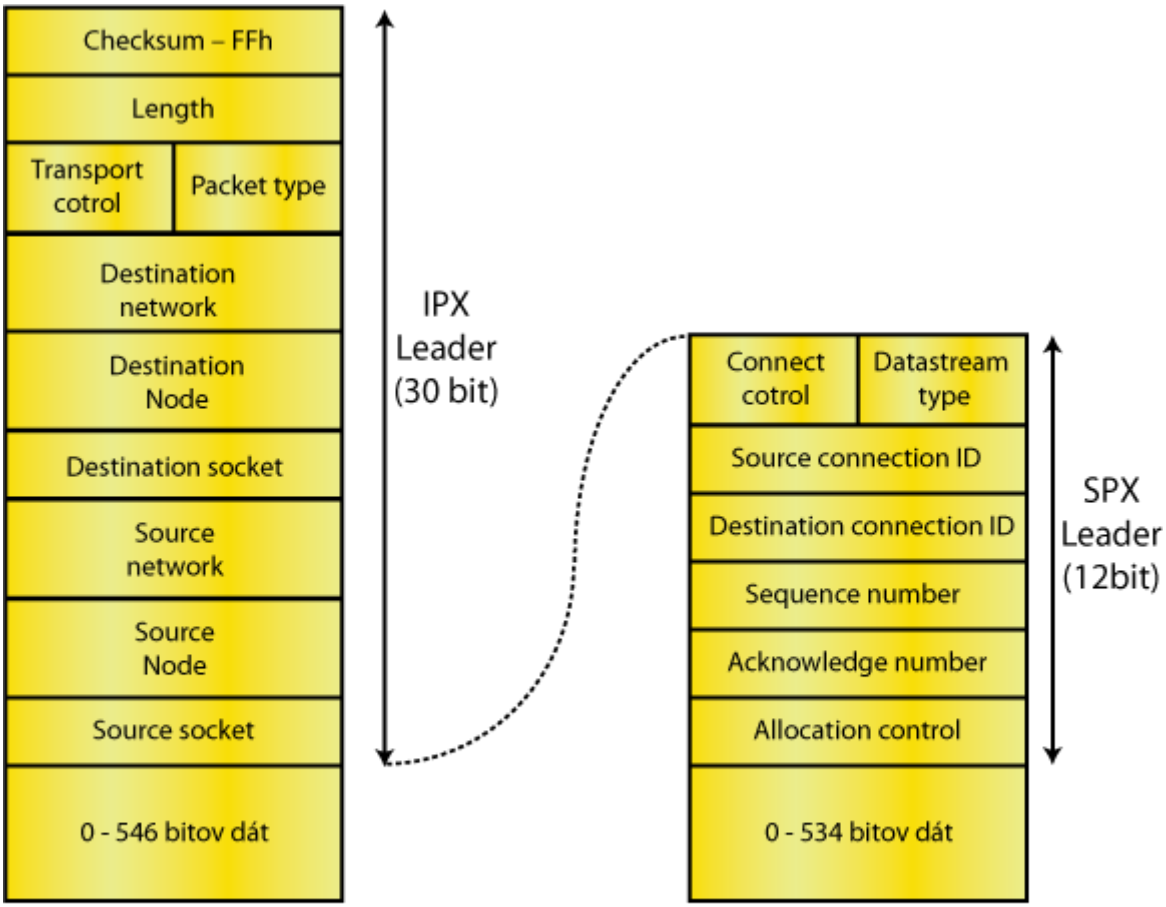
7.2.1 Protokoly NetBIOS a NetBEUI

Najstarším sieťovým protokolom určeným špecificky pre prostredie lokálnej siete (kde existuje možnosť, aby rámec odosielaný jednou zo staníc siete bol prijatý všetkými ostatnými stanicami), je **NetBIOS** navrhnutý firmou IBM. Aplikácia sa identifikuje menom a protokol pre správu NetBIOSu sa stará o jedinečnosť tohto mena v sieti. NetBIOS bol priamo viazaný na ovládač komunikačného radiča. Rovnakým spôsobom je implementovaný v LAN Manager, kde je rozšírený, doplnený používateľsky lepším rozhraním a pomenovaný **NetBEUI** (NetBIOS Extended User Interface).

Aplikácia musí pre vyžiadanie funkcie NetBIOSu pripraviť požiadavkový blok **NCB** (Network Control Block), v ktorom zadáva parametre volania - mená, číslo logického kanálu, adresu a dĺžku predávaných dát, časové limity pre vysielanie a príjem. Požiadavky odovzdá aplikácii NetBIOSu volaním systému (prerušenie 5C H). Po odovzdaní požiadaviek môže aplikácia pokračovať vo svojej činnosti. Ukončenie požiadavky môže aplikácia aktívne testovať alebo môže ukončením požiadavky aktivovať dokončovaciu rutinu. Komunikujúce aplikácie (alebo jej komunikačné kanály) sú identifikované menami, ktoré majú dĺžku 16 znakov. Meno môže byť buď individuálne (a jedinečné v určitej sieti) alebo skupinové. Základná služba, ktorú NetBIOS podporuje, je datagramová služba (pri protokole NetBEUI jej zodpovedá služba *MailSlot*), dovoľujúca odovzdanie správy o dĺžke do 512 bytov jednému adresátovi alebo ľubovoľnej stanici na sieti, ktorá takú správu očakáva (Broadcast). Virtuálne kanály (u NetBIOSU relácie, u NetBEUI služba Named Pipes) dovoľujú prenášať správy o dĺžke 131071 znakov, ktoré sú pri prenose delené do paketov. Na ďalšom obrázku je štruktúra paketov protokolu NetBIOS.

7.2.2 Protokol IPX/SPX

S protokolmi **IPX/SPX** (Internet Packet eXchange/Sequential Packet eXchange) komunikuje sieťový operačný systém Novell Netware. Protokoly vychádzajú zo systému **XNS** (Xerox Network System), ktorý bol alternatívou firmy Xerox k protokolom TCP/IP. Protokol *IPX* zaisťuje prenos paketov bez potvrdzovania medzi aplikáciami pripojenými na zvolené pripojovacie miesta (Socket). Protokol *SPX* je nadstavbou protokolu IPX, zaisťuje potvrdzovanie prenesených paketov a umožňuje prácu viacerých aplikačných procesov na jednom porte. Komunikačné funkcie IPX/SPX vyžadujú, aby aplikácia uložila potrebné parametre do požiadavkového bloku **ECB** (Event Control Block), obsluha požiadaviek môže byť asynchrónna k ďalšiemu behu aplikácie. Aplikácia môže na ukončenie požadovanej funkcie aktívne čakať alebo môže byť prerušená dokončovacou rutinou. Nasledujúci obrázok ukazuje štruktúru paketov protokolov IPX a SPX.

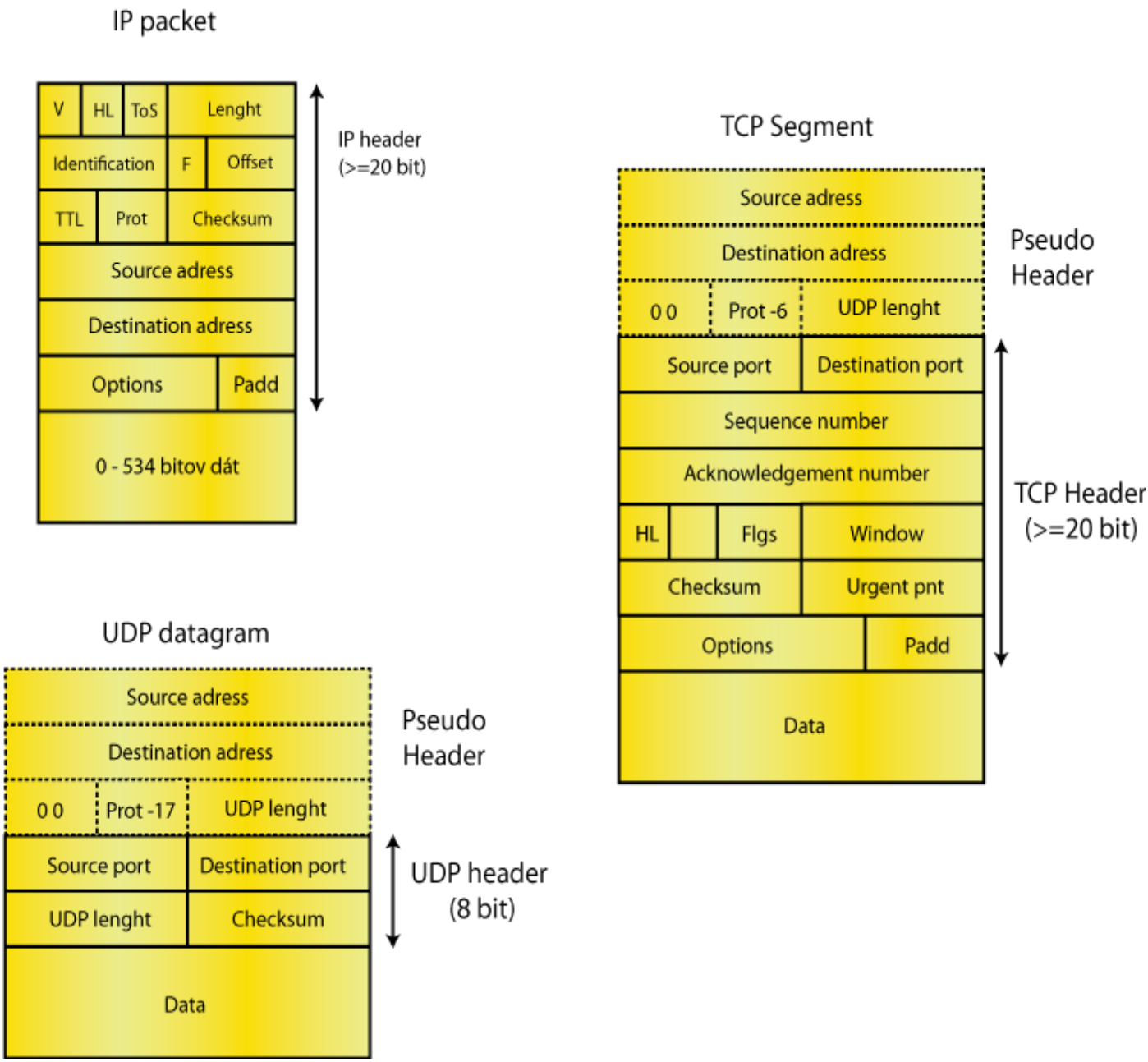


Pakety protokolov IPX a SPX

Výhodou protokolov IPX/SPX je adresácia, ktorá vychádza z adresácie staníc v lokálnej sieti. Adresa je v IPX definovaná ako dvojica (32bitová adresa siete, 48bitová adresa stanice), to zjednodušuje prácu smerovačov, ale i staníc v sieti. Podstatnou nevýhodou IPX/SPX je skutočnosť, že adresu siete definuje správca konkrétnej siete. Chýbajúce kooperácie v prideľovaní adries v princípe znemožňuje vzájomné prepojenie sietí protokolmi IPX/SPX medzi sebou.

7.2.3 Protokol TCP/IP

Protokoly **TCP/IP** sú v súčasnosti akceptované ako štandard pre komunikáciu v rozsiahlych počítačových sietiach. Architektúra TCP/IP zahŕňa vlastný prenos paketov *IP* (Internet Protocol), jednoduché datagramové rozhranie **UDP** (User Datagram Protocol) a protokol logického kanálu **TCP** (Transmission Control Protocol). Protokol TCP zaisťuje potvrdzovanie v prostredia prepojených sieťou, v ktorých môžu byť pakety dodávané v nezaručenom poradí, môžu byť štiepené na *fragmenty* a môžu sa strácať. Je vybavený dômyselným riadením toku a ochranou proti chybám, vyvolaným opakovaným naväzovaním spojenia. Aplikáciám sú viditeľné protokoly IP, UDP a TCP podporované služobnými protokolmi, ktoré zaisťujú transformácie adries TCP/IP na adresy lokálnej siete (ARP, RARP), riadenie siete (ICMP) a podporu smerovania (RIP, OSPF). Aplikačné rozhrania protokolov TCP, IP a UDP sú pomerne presne definované v systémoch UNIX, ako *BSD sokety* (BSD Sockets) alebo ako rozhranie *TLI* (Transport Layer Interface). Rozhranie v systémoch Windows je obdobou BSD soketov, doplnené o podporu asynchrónneho výkonu funkcií. Funkcie rozhrania zahŕňajú vytváranie (Socket) a rušenie (Close) dátových štruktúr riadiacich komunikácií na danom prípojnom mieste (portu) alebo po virtuálnom kanále, ich väzbu na logický kanál, väzbu na adresačnú informáciu (Bind) a limit počtu neobslúžených požiadaviek na vstupe (Listen). Súčasťou rozhrania TCP sú funkcie pre pasívne a aktívne otvorenie kanálu (Accept a Connect) a pre jeho uzatvorenie (Close). Prenos paketov a správ zaisťujúc volanie funkcií Write a Read, spolu s niekoľkými formami funkcií Send a Receive. Formát IP paketov, UDP datagramov a TCP segmentov je na nasledujúcom obrázku.

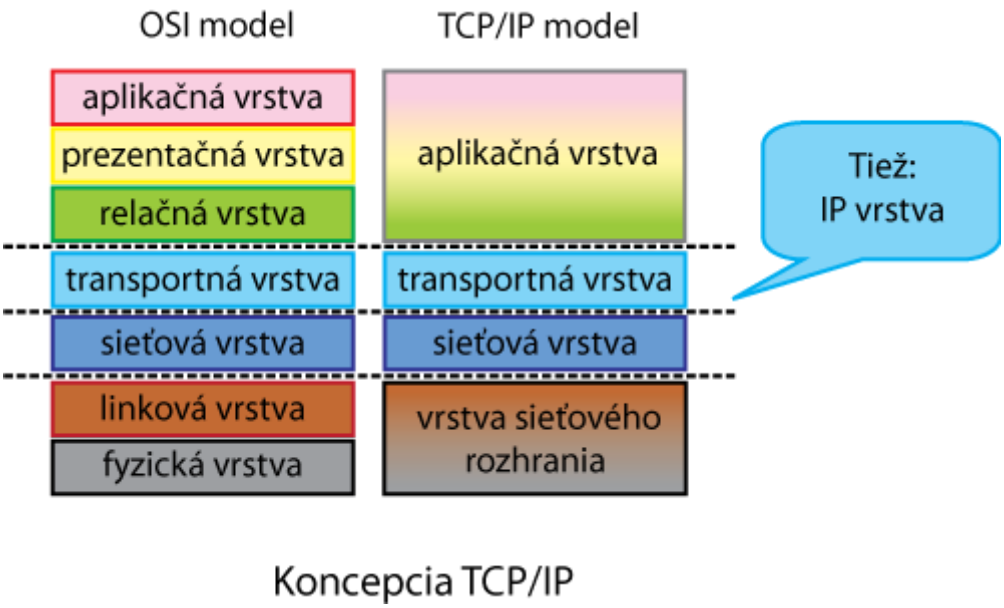


TCP/IP je v skutočnosti sieťová architektúra, ktorá obsahuje ucelenú predstavu o počte a úlohe vrstiev a obsahuje i konkrétne protokoly. História vzniku TCP/IP súvisí s Internetom (ARPANETem) postaveným na „dočasnej“ paketovej technológii NCP (Network Control Protocol). Cieľom bolo overiť životaschopnosť paketovej technológie. Pretože protokol NCP nebol vhodný pre rutinné používanie bol TCP/IP vyvíjaný ako „definitívne“ riešenie pre vznikajúci Internet. Filozofia, uplatnená pri vzniku TCP/IP, vychádzala ešte z pôvodných požiadaviek na ARPANET (ktorý bol navrhnutý pre vojakov), že nesmie mať žiadnu centrálnu časť (tú by nepriateľ zničil ako prvú). Charakterom musí byť prevažne decentralizovaný, musí

to byť veľmi robustné (tak aby to aspoň nejako fungovalo, keď nepriateľ časť siete odstrelí) a komunikácia bude mať nespojovaný charakter. Filozofia TCP/IP je riešená tak, aby išlo ľahko pripojovať samostatné siete a rôzne sieťové technológie. Požiadavkou bolo, aby prenosová časť hlavne prenášala dáta a nestarala sa o ďalšie veci a spoľahlivosť si zaistili až koncové uzly a nikdy prenosová časť siete. Preto prenosová časť (sieťová vrstva) funguje iba nespoľahlivo a mechanizmy zaisťujúce spoľahlivosť sú implementované až v transportnej vrstve (ale ako voliteľná možnosť - tj. Nie je povinnosť ich využívať). Otázkou je, prečo je výhodnejšie, aby si spoľahlivosť zaisťovali až koncové uzly. Niektoré aplikácie nemusia spoľahlivosť potrebovať

a dajú prednosť rýchlemu a pravidelnému prenosu. Spoľahlivosť je vždy relatívna (nikdy 100%), niekomu by nemusela postačovať miera „zabudovanej“ spoľahlivosti a musel by si ju zaisťovať sám a znovu a to by bolo neefektívne, pretože réžia by sa sčítala. Pretože k zaisteniu spoľahlivosti je potrebná výpočtová kapacita a tá je

lacnejšia v koncových uzloch než vo „vnútri“ siete, autori TCP/IP sa nespoľahlivých služieb nebáli. Filozofia, uplatnená pri vzniku TCP/IP, to znamená 52maximálnu robustnosť vedľa k nespojovanému charakteru, aby pri výpadku nebolo nutné zložito rušiť stávajúci a naväzovať nové spojenia. Komunikácia by mala mať skôr bezstavový charakter (aby sa nemusela uchovávať žiadna stavová informácia o doterajšom priebehu komunikácie) tzn., aby nebolo nutné sa zložite zotavovať z prípadného výpadku. Ďalšou filozofiou, uplatnenou pri vzniku TCP/IP, je zdieľanie mechanizmov. TCP/IP to rieši tak, aby réžiu neniesli tí, ktorí ich nechcú používať, tzn. nie zdieľane. Zabudovávajú sa priamo a iba do tých aplikácií, ktoré ich skutočne potrebujú. Réžiu nenesie ten, kto mechanizmy nepotrebuje. Koncepcia vrstiev TCP/IP je zrejmá z obrázka.



Koncepcia TCP/IP

Aplikačná vrstva TCP/IP má koncepciu podobnú aplikačnej vrstve ISO/OSI. Sú tu základné časti aplikácií, ostatné (UI) sú nad aplikačnou vrstvou. Služby relačného a prezentačného charakteru sú priamou súčasťou aplikácií. Pôvodné služby aplikačnej vrstvy sú: elektronická pošta, prenos súborov a vzdialené prihlasovanie. Neskôr vznikajú

ďalšie ako: zdieľanie súborov, správa siete, sprístupnenie informácií, WWW.

Transportná vrstva TCP/IP ri eši komunikáciu koncových účastníkov (end-to-end communication). Sama využíva nespojovaný a nespoľahlivý prenos na úrovni sieťovej vrstvy. Alternatívne ponúka spojovaný a spoľahlivý prenos a aplikácie si môžu vybrať podľa vlastného uváženia. Protokol TCP (Transmission Control Protocol) zaisťuje spoľahlivý a spojovaný prenos, „tvári sa“ ako prúd (stream), ktorý prenáša jednotlivé byty. Protokol UDP (User Datagram Protocol) zaisťuje nespojovaný a nespoľahlivý prenos a je len „ľahkou nadstavbou“ nad sieťovou vrstvou, nemení povahu prenosových služieb sieťových vrstiev.

Sieťová vrstva TCP/IP zaisťuje iba nespojovaný a nespoľahlivý prenos tj. „holé minimum“, ale snaží sa byť čo najrýchlejšia. Zaisťuje jednotné prenosové služby nad všetkými možnými prenosovými technológiami nižších vrstiev, vytvára „jednotnú striešku“ .

Protokol IP (Internet Protocol) je hlavný (a jediný) prenosový protokol, snaží sa zakrývať špecifiká prenosových technológií nižších vrstiev a fungovať nad nimi optimálne. Sú varianty ako SLIP (Seriál Line IP), PPP (Point-to-point protokol).

Vrstva sieťového rozhrania (Network Interface Layer) zahŕňa „všetko pod sieťovou vrstvou“. TCP/IP túto vrstvu samé nijak nenapĺňa, tj. nešpecifikuje svoje vlastné prenosové technológie na najnižších vrstvách. Predpokladá sa, že tu sa použije to, čo vznikne niekde inde (mimo rámec TCP/IP), napríklad Ethernet, Token Ring, ATM. TCP/IP sa zaoberá iba tým, ako tieto technológie čo najlepšie využiť, ako nad nimi prevádzkovať IP. Snaha prekryť odlišné prenosové technológie jednotnou „strieškou“ naráža na problémy s adresami. Napr. Ethernet používa 48-bitové adresy, ARCnet 8-bitové atď. (tj. linkové adresy sú veľmi odlišné). Protokol IP používa 32-bitové adresy (tzv. IP adresy). Protokol IP sám dáta fyzicky neprenášajú (ale využíva tie prenosové technológiie, ktoré sú „pod ním“). Služby „pod“ protokolom IP môžu byť rôznorodé, hlavne z hľadiska:

- veľkosti prenášaných blokov (rámcov),
- miery spoľahlivosti,
- prenosového oneskorenia,
- spojovaného či nespojovaného charakteru,
- charakteru prenosu (dá sa robiť broadcasting?).

Protokol IP sa zameriava na „holé minimum“. Štandardy TCP/IP sú skutočne otvorené, i keď nikto poriadne nevie, čo to presne znamená. Nie sú „v rukách“ jedinej firmy, vznikajú (sú prijímané) na základe všeobecného konsensu , špecifikácie týchto protokolov sú verejným vlastníctvom, za ich využitie sa neplatia žiadne licenčné poplatky, texty špecifikácií majú povahu voľne šíriteľných dokumentov (dokumentov RFC). Štandardy vznikajú v rámci „združenia“ IETF (Internet Engineering Task Force) čo je dosť voľné spoločenstvo odborníkov, zainteresovaných na vývoji TCP/IP. Nad IETF stojí „dozorná rada“, IESG (Internet Engineering Steering Group) ktorá riadi prácu jednotlivých skupín v rámci IETF a nad IESG stojí IAB (Internet Architecture Board), ktorá vydáva vlastné štandardy . V súčasnosti vlastné technické riešenia vznikajú skôr

Vo firmách a firmy predkladajú svoje riešenie k IETF. Keď je riešenie uznané za potrebné a vhodné, môže byť prijaté ako štandard Internetu a tým sa štandardizované riešenie stáva „verejným vlastníctvom“. Každý štandard má formu dokumentu RFC (Request for Comment). V súčasnosti existujú rádovo tisíce dokumentov RFC, avšak nie všetky dokumenty RFC sú štandardy!!!! Väčšina má povahu informačných materiálov, návodov, odporučení. Dokumenty RFC sú voľne šíriteľné a nikdy sa nemenia, ich obsah zostáva vždy rovnaký, dá sa ich ľahko archivovať a šíriť nikdy nevznikajú neaktuálne verzie a keď je potrebné nejaké riešenie zmeniť, vydá sa nový dokument RFC a ten vo svojej hlavičke prehlási predchádzajúci dokument RFC za „prežitý“ (obsolete). K jednej a tej istej

problematike sa v rôznych okamihoch môžu vzťahovať rôzne dokumenty RFC. Každý dokument STD sa vždy vzťahuje k určitej konkrétnej problematike. Obsahom dokumentu STD je ten dokument RFC, ktorý v danom okamihu rieši príslušnú problematiku. Koncepcia protokolov TCP/IP vznikla v rokoch 1977-8. Internet prešiel na TCP/IP od 1.1.1983 a od tej doby sa koncepcia principiálne nezmenila. Ďalší vývoj má charakter zdokonaľovania a obohacovania, pribúdajú hlavne nové služby ako NFS Gopher, WAIS, WWW a ďalšie. Doterajšie služby sa obohacujú o ďalšie možnosti napr. el. pošta podporu netextových formátov (štandard MIME). V poslednom období je TCP/IP silne kritizovaný a to z niekoľkých pohľadov:

- Internet nie je bezpečný, lebo protokoly TCP/IP nezaisťujú takú mieru bezpečnosti, akú by si (niektorí) používatelia predstavovali. Je však faktom, že pri vzniku koncepcie TCP/IP nebola požiadavka zabezpečenia vznesená a autori sa sústredili hlavne na efektívnosť prenosov. Malá miera bezpečnosti spočíva v tom, že prenášané dáta nie sú šifrované, ani inak zabezpečené proti odposluchu a zneužitiu. Protokol IP nijak nešifruje to, čo prenáša. V dobe akademického Internetu malá úroveň bezpečnosti nevadila, avšak v dobe komerčného využitia to vadí veľmi! Zmena by znamenala úpravu protokolu IP. Už dnes ale existujú možnosti zvýšenia miery zabezpečenia a to šifrovaním na aplikačnej úrovni kde si aplikácia sama zabezpečí dáta ešte pred ich odosielaním. Iný spôsob je pomocou zabezpečených tunelov, kedy sa vytvárajú zabezpečené virtuálne kanály (tunely) a prenášané dáta (IP pakety) sa zašifrujú, vložia do normálnych IP paketov a takto prenesú.
- Filozofia TCP/IP nepočíta s mobilitou používateľov, tzn., že sa nedá mať jednu IP adresu a cestovať s ňou po svete. IP adresy sú viazané na „geografické“ (topologické) umiestnenie. Priame využitie mobilných komunikačných technológií je problematické, napr. GSM (musí sa obchádzať tým, že sa GSM využíva rovnako ako bežná telefónna sieť).
- Nedostatok adries, kedy autori TCP/IP zvolili 32-bitový adresový priestor (IP adresy sú 32-bitové). Pritom autori pamätali na existenciu rôzne veľkých sietí, ktoré potrebujú rôzne počty adries a vznikli triedy A, B, C, ... Pôvodný spôsob prideľovania adries

z tohoto adresového priestoru nebol príliš hospodárny. Autori ani tak neurobili chybu, ako skôr nedocenili obrovitosť svojho úspechu, neodhadli, aký ohromný záujem bude

o pripájanie k Internetu. Problémom je hroziace vyčerpanie IP adries, ktorý sa začal riešiť dočasnými opatreniami, ktoré majú za úlohu spomaliť úbytok adries. Tým je mechanizmus CIDR (rieši i ďalšie problémy) tzv. privátne IP adresy. Zásadným koncepčným riešením, ktoré by problém definitívne odstránilo, je nájdenie novej verzie protokolu IP (IPnG, IP next Generation, resp. IPv6).

- Charakter prenosu - prenosové protokoly TCP/IP sú orientované na prenos el. pošty, súborov apod., majú „dávkový“ (nárazový) charakter, negarantujú za akú dobu sú údaje doručené, ani s akou pravidelnosťou budú doručované jednotlivé časti dát. To veľmi vadí multimediálnym prenosom, prenosom živého zvuku a obrazu. Zvyšovaním prenosových kapacít je možné nepriaznivý efekt zmierniť, ale nie odstrániť celkom. Vďaka tomu sa stalo možné napr. telefonovanie cez Internet. Riešením sú až špecializované prenosové protokoly, podporujúce prenos v reálnom čase RTP a RSVP.

7.2.4 Porovnanie TCP/IP a referenčného modelu ISO/OSI

● ISO/OSI a jeho súčasti vznikajú štýlom „od zložitého k jednoduchšiemu“, najprv sa požaduje veľa a potom sa musí uberať. Vznikajú problémy s kompatibilitou „podmnožín“. K prijatiu štandardu nie je potrebné overenie praktickej realizovateľnosti. Naopak TCP/IP vzniká štýlom „od jednoduchého k zložitejšiemu.“ Najprv sa prijme jednoduchšie riešenie, potom sa ev. pridáva. Existuje záruka kompatibility aspoň na úrovni „spoločného minima.“ Pre prijatie štandardu je nevyhnutné overenie praktickej realizovateľnosti, dokonca i praktické predvádzanie skúsenosti.

● Štandardy ISO sa predávajú a sú naozaj veľmi drahé. Uplatňuje sa stratégia: *„chcem aby si dodržiaval moje štandardy a musíš mi najprv veľa zaplatiť, aby som ti vôbec povedal v čom spočívajú“ a* výsledok tomu zodpovedá. Naopak štandardy TCP/IP (i súvisiace dokumenty) sú dostupné voľné a zadarmo. Uplatňuje sa stratégia: *„keď chcem niečo presadiť, musím k tomu maximálne uľahčiť prístup“* a táto stratégia funguje.

● Referenčný model ISO/OSI je vhodný ako model pre štúdium sietí a to s vynechaním relačnej a prezentačnej vrstvy sú protokoly „ušité na mieru“ sieťovému modelu. Pre praktické použitie je len veľmi málo vhodný. Naopak TCP/IP je výhodný pre praktické použitie, ako model pre štúdium sietí už nie je až tak výhodný, sieťový model TCP/IP je „ušiť na mieru“ konkrétnym protokolom.

Precvičte sa

Kontrolné otázky:

7.1. Aké sú základné koncepčné odlišnosti modelu ISO/OSI a TCP/IP?

Úlohy na zamyslenie:

7.1. Prečo sa vo väčšine sieťových modelov používa rozdelenie do vrstiev?

7.2. Čím je rozdelenie do vrstiev špecifické a odlišné od iných spôsobov dekompozície systémov?

7.3. Čo považujete za najdôležitejší faktor, ktorý viedol k tomu, že sa v praxi výrazne viac rozšíril model TCP/IP, než RM ISO/OSI?

Korešpondenčná úloha:

7.1. Akú fyzickú topológiu má Vami najčastejšie používaná počítačová sieť? Pokúste sa nakresliť jej schému.

7.2. Viete s ktorými metódami riadenia prístupu k médiu pracujú Vami používané siete? Pokiaľ nie, pokúste sa to zistiť napr. u správcu siete.

Z hrnutie obsahu kapitoly

V tejto kapitole sa študenti zoznámili s referenčným modelom počítačovej siete ISO/OSI a jeho základnými vlastnosťami. Študenti sa zoznámili s princípom rozdelenia funkcií obecnej počítačovej siete do vrstiev, s názvami a funkciami jednotlivých vrstiev referenčného modelu, od prvej vrstvy fyzickej až po poslednú, aplikačnú. V tejto kapitole sa tiež študenti zoznámili s najdôležitejšími protokolmi prakticky používanými v počítačových sietiach. Jedná sa o protokol NetBIOS a jeho rozšírenie NetBEIU, ďalej protokolovú sadu SPX/IPX a hlavne rodinu protokolov TCP/IP, ktorá sa v posledných niekoľkých rokoch veľmi rýchlo rozširuje a stáva sa prakticky štandardnou protokolovou sadou, pre komunikáciu vo všetkých typoch sietí. Preto bol tiež protokolovej sade TCP/IP venovaný v tejto kapitole najväčší priestor, zoznámili sme sa teda s históriou TCP/IP, jej štandardami, vrstevnatou štruktúrou a aktuálnymi problémami.