UNIVERZITA PARDUBICE

DOPRAVNÍ FAKULTA JANA PERNERA

BAKALÁŘSKÁ PRÁCE

2020 Ivo Seemann

Univerzita Pardubice

Dopravní fakulta Jana Pernera

Studijní pomůcka – Základy počítačových sítí

Bakalářská práce

2020 Ivo Seemann

Univerzita Pardubice
Dopravní fakulta Jana Pernera
Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Ivo Seemann**
Osobní číslo:	**D17205**
Studijní program:	**B3709 Dopravní technologie a spoje**
Studijní obor:	**Aplikovaná informatika v dopravě**
Téma práce:	**Studijní pomůcka – Základy počítačových sítí**
Zadávající katedra:	**Katedra informatiky v dopravě**

Zásady pro vypracování

Cílem práce je vytvoření podkladového materiálu pro úvod do problematiky počítačových sítí pro nově příchozí pracovníky na pracoviště CIS u VÚ 7214 Čáslav.
Bakalářská práce se zaměří na vytvoření studijní pomůcky pro nově příchozí pracovníky. Práce bude mít tři hlavní části:

- V první části bude práce zaměřena na historii, vývoj, topologii a základní principy fungování počítačových sítí.
- V druhé části bude vysvětlovat protokoly IPv4 a IPv6, IP adresu a směrování.
- Třetí část bude zaměřena na základní komponenty počítačových sítí.

Rozsah pracovní zprávy: **30 normostran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. ODOM, Wendell. *Počítačové sítě bez předchozích znalostí.* 1. vyd. Brno : CP Books, a.s., 2005. 384 s. ISBN 80-251-0538-5.
2. PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z : technologie pro datovou, hlasovou i multimediální komunikaci.* 2. aktualiz. vyd. [s.l.] : [s.n.], 2006. 430 s. ISBN 80-251-1278-0.
3. *Cisco Networking Academy Program: CCNA 1 and 2 Lab Companion.* USA: Cisco Press, 2003.
4. *EArchiv.cz: Archiv článků a přednášek Jiřího Peterky* [online]. 2019 [cit. 2019-11-28]. Dostupné z:www.earchiv.cz

Vedoucí bakalářské práce: **Ing. Zdeněk Drvota**
Katedra informatiky v dopravě

Datum zadání bakalářské práce: **28. listopadu 2019**
Termín odevzdání bakalářské práce: **22. května 2020**

L.S.

doc. Ing. Libor Švadlenka, Ph.D.
děkan

doc. Ing. Karel Greiner, Ph.D.
vedoucí katedry

V Pardubicích dne 28. listopadu 2019

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 23.6. 2020

Ivo Seemann

Poděkování

Na tomto místě bych chtěl poděkovat vedoucímu bakalářské práce Ing. Zdeňku Drvotovi za cenné rady, věcné připomínky, vstřícnost při konzultacích a vypracování bakalářské práce. Mé poděkování patří též mé rodině za pomoc a podporu během studia.

Anotace

Cílem této práce je vytvoření podkladového materiálu pro úvod do problematiky počítačových sítí. Práce je rozdělena do tří teoretických částí. První část se zabývá historií a vývojem počítačových sítí. Vysvětluje rozdíl mezi ISO/OSI modelem a TCP/IP architekturou. Druhá část je zaměřena na adresaci a směrování. Popisuje protokoly IPv4 a IPv6 a základy směrovacích protokolů RIP, IGRP, EIGRP a OSPF. Třetí část se zabývá pasivními a aktivními prvky sítě.

Klíčová slova

počítačová síť, paket, ISO/OSI, TCP IP, topologie, Ethernet, IPv4, IPv6, směrování

Title

Study aid – Basics of computer networks

Annotation

The aim of this bachelor's thesis is to create background material for an introduction to computer networks. The work is divided into three theoretical parts. The first part deals with the history and development of computer networks. Explains the difference between the ISO / OSI model and the TCP / IP architecture. The second part is focused on addressing and routing. Describes IPv4 and IPv6 protocols and the basics of RIP, IGRP, EIGRP, and OSPF routing protocols. The third part deals with passive and active network elements.

Keywords

computer network, packet, ISO / OSI, TCP IP, topology, Ethernet, IPv4, IPv6, routing

Obsah

Seznam obrázků 9
Úvod 10
1 Historie 11
2 Modely a architektura počítačových sítí 15
2.1 Architektura počítačových sítí 16
2.2 Referenční model ISO OSI 16
2.2.1 Fyzická vrstva 17
2.2.2 Linková vrstva 18
2.2.3 Síťová vrstva 18
2.2.4 Transportní vrstva 19
2.2.5 Relační vrstva 21
2.2.6 Prezentační vrstva 22
2.2.7 Aplikační vrstva 23
2.3 TCP IP 23
2.3.1 Vrstva síťového rozhraní 25
2.3.2 Síťová vrstva 25
2.3.3 Transportní vrstva 27
2.3.4 Aplikační vrstva 27
3 Rozdělení sítí a standardy sítí LAN 28
3.1 Rozdělení dle rozlohy sítě 28
3.1.1 Sítě PAN 28
3.1.2 Sítě LAN 28
3.1.3 Sítě CAN 28
3.1.4 Sítě MAN 28
3.1.5 Sítě WAN 29
3.1.6 Sítě GAN 29
3.2 Topologie sítí 29
3.2.1 Fyzická topologie 29
3.2.1.1 Dvoubodové spojení 30
3.2.1.2 Sběrnicová topologie 30
3.2.1.3 Kruhová topologie 30
3.2.1.4 Topologie hvězdy 31

3.2.1.5 Stromová topologie 32
3.2.1.6 Síť se smyčkami 33
3.2.2 Logická topologie 33
3.3 Rozdělení dle metody přístupu k médiu 33
3.3.1 CSMA/CD 34
3.3.2 Token ring 34
3.3.3 Token bus 34
3.4 Standardy sítí LAN 34
3.4.1 Ethernet (802.3X) 35
3.4.1.1 Ethernet (10BASE-X) 36
3.4.1.2 Fast Ethernet (100BASE-X, IEEE 802.3u, y) 36
3.4.1.3 Gigabit Ethernet (1000BASE-X, IEEE802.3z, ab) 37
3.4.1.4 10GB Ethernet (IEEE802.3ae) 37
3.4.2 Token Ring (802.5) 38
4 Adresace v síti 40
4.1 Fyzické adresy 40
4.2 Logické adresy 40
5 IPv4 41
5.1 Rozdělení IP adres 41
5.1.1 Adresy třídy A 42
5.1.2 Adresy třídy B 42
5.1.3 Adresy třídy C 43
5.1.4 Adresy třídy D 43
5.1.5 Adresy třídy E 44
5.2 Tvorba podsítí 44
5.2.1 Tvorba podsítí pomocí masky s pevnou délkou 44
5.2.2 Tvorba podsítí pomocí masky s proměnnou délkou VLSM 45
5.3 CIDR 45
5.4 Neveřejné adresy 46
5.5 NAT 46
6 IPv6 48
6.1 Adresa IPv6 48
6.2 ICMPv6 50

6.2.1 Chybové zprávy 51
6.3 DNS 51
6.3.1 Dopředné dotazy 51
6.3.2 Zpětné dotazy 51
7 Směrování 52
7.1 Statické směrování 52
7.2 Dynamické směrování 53
7.2.1 Směrovací protokol RIP 54
7.2.2 Směrovací protokol IGRP 55
7.2.3 Směrovací protokol EIGRP 55
7.2.4 Směrovací protokol OSPF 56
8 Přenosová média 58
8.1 Koaxiální kabel 58
8.1.1 Tenký koaxiální kabel 58
8.1.2 Tlustý koaxiální kabel 58
8.2 Symetrický kabel (kroucená dvojlinka) 58
8.2.1 Symetrický kabel nestíněný 59
8.2.2 Symetrický kabel stíněný 59
8.2.3 Kategorie symetrického kabelu 59
8.3 Optický kabel 60
8.3.1 Single mode optické vlákno 60
8.3.2 Multimode optické vlákno 60
8.4 Bezdrátové připojení 60
9 Síťová zařízení 62
9.1 Repeater 62
9.2 Media konvertor 62
9.3 Switch 62
9.4 Router 63
9.5 Gateway 63
10 Závěr 64
11 Bibliografie 65

Seznam obrázků

Obrázek 1 – Horizontální komunikace mezi vrstvami [37] 15
Obrázek 2 – Sedm vrstev RM ISO OSI [38] 17
Obrázek 3 – Hlavička protokolu TCP [39] 20
Obrázek 4 – Hlavička protokolu UDP [40] 21
Obrázek 5 – Vztah relace a transportního spojení [41] 22
Obrázek 6 – Srovnání vrstev RM ISO OSI a TCP IP [42] 24
Obrázek 7 – Protokoly a vrstvy TCP IP [43] 24
Obrázek 8 – Protokol RARP [45] 26
Obrázek 9 – Protokol ARP [44] 26
Obrázek 10 – Sběrnicová topologie 30
Obrázek 11 – Kruhová topologie 31
Obrázek 12 – Topologie hvězdy 32
Obrázek 13 – Stromová topologie 32
Obrázek 14 – Topologie částečný mesh 33
Obrázek 15 – Architektura IP adresy třídy A 42
Obrázek 16 – Architektura IP adresy třídy B 43
Obrázek 17 – Architektura IP adresy třídy C 43
Obrázek 18 – Architektura IP adresy třídy D 43
Obrázek 19 – Formát IP adres pomocí tříd a v rámci CIDR 46
Obrázek 20 – Datagram IPv6 s ICMPv6 50

Úvod

V dnešní době nabyté technologiemi, jakými je například virtuální realita , internet a mnoho dalších, se počítačové sítě stali naší každodenní součástí ať už si to uvědomujeme či nikoli. Využíváme je jak v osobním, tak i v pracovním životě. Díky těmto sítím jsme například schopni se informovat o aktuálním počasí, zjistit odjezdy a příjezdy dopravních prostředků, nakupovat veškeré dostupné zboží, provádět bankovní transakce. Počítačové sítě nám zpřístupnily neomezený zdroj zábavy a informací v podobě celosvětové sítě, která se nazývá internet. Toho, co vše nám počítačové sítě umožňují je nepřeberné množství.

Abychom mohli všech těchto poskytovaných služeb využít, je zapotřebí odborníků, kteří se starají o vývoj, výstavbu a údržbu těchto sítí. To však od těchto lidí vyžaduje určitý druh povědomí a vzdělání v oboru zabývajícím se počítačovými sítěmi. Aby bylo možné se v tomto oboru vzdělávat, je nejprve zapotřebí pochopení základních principů počítačových sítí. A právě těmito základy se tato práce zabývá.

Hlavním účelem této práce je přiblížit základy počítačových sítí pro nově příchozí pracovníky na pracoviště komunikačních a informačních technologií u VÚ7214 Čáslav. Práce není plnohodnotnou učebnicí, ale podpůrným studijním materiálem, který výše uvedeným pracovníkům pomůže při jejich dalším vzděláváním v tomto oboru. Práce je rozdělena do tří na sebe navazujících částí.

První část je zaměřena na vznik a vývoj počítačových sítí. Dále je zde představen RM ISO OSI a architektura TCP IP a jejich jednotlivé vrstvy. V dalších kapitolách je popisována topologie, jednotlivé standardy sítí LAN a způsob adresace v těchto sítích. Druhá část je zaměřena na protokoly IP jak ve verzi 4 tak ve verzi 6. Poslední kapitola druhé části je věnována základům směrování a směrovacích protokolů. Třetí část této práce se zabývá stručným popisem aktivních a pasivních prvků počítačových sítí.

1 Historie

První myšlenky na vytvoření a využití počítačové sítě sahají do období těsně po druhé světové válce. V tomto období probíhala mezi USA a tehdejším SSSR studená válka. Tyto mocnosti se předháněly ve zbrojení, především ve vývoji jaderných zbraní. V důsledku toho USA v padesátých letech minulého století budují zcela nový systém protivzdušné obrany, který je založen na propojení radarových stanic. Systém má být schopen zachytit blížící se ruské bombardéry přepravující atomové bomby.

Tento systém protivzdušné obrany, nazývaný SAGE (*Semi-Automatic Ground Environment*), je možno považovat za jednu z prvních počítačových sítí na světě. Byl tvořen 23 počítačovými centry a 100 radarových stanic. Informace mezi těmito stanicemi a centry byly přenášeny skrze telefonní linky, a to v reálném čase. V každém centru se nacházely dva počítače AN/FSQ-7 od firmy IBM, z nichž jeden byl v provozu a druhý sloužil jako záloha. [1] [2] Nevýhodu tohoto systému byla právě tato centra. Pokud by došlo ke zničení jednoho z center, dojde k následné ztrátě informací z radarových stanic připojených k tomuto centru. Později z tohoto systému firma IBM vytvořila komerční verzi nazvanou SABER (*Semi-Automatic Business-Related Environment*), která sloužila jako rezervační systém sedadel v letadlech American Airlines. [3] Jednalo se o úplně první komerční síť fungující v reálném čase.

Na začátku šedesátých let si USA uvědomily zranitelnost systému SAGE a zadaly firmě RAND (*Research And Development*) Corporation vytvořit systém pro komunikaci mezi jednotlivými ministerstvy a institucemi vlády USA s důrazem kladeným na fungování za jakýchkoli podmínek. [4] V roce 1964 firma představila řešení, které bylo založeno na dvou základních principech. První princip spočíval v decentralizaci. To znamená, že síť nemá žádné řídící centrum, a tudíž všechny její uzly jsou si rovny. Druhým bylo zajištění přenosu informace i přes nefunkčnost některého z uzlů. Tento požadavek stál u zrodu myšlenky na přenos informací po částech, takzvaných paketech. Každý z těchto paketů bude navíc obsahovat adresu příjemce a bude cestovat nezávisle na ostatních paketech po různých cestách. Tento způsob přenosu informací byl nazván jako přepojování paketů (*packet switching*). [5] [6] Na základě těchto dvou principů byla počítačová síť poprvé implementována ve Velké Británii v roce 1968. Jednalo se o experimentální síť Národní laboratoře pro fyziku. V USA se s touto sítí začíná experimentovat o rok později. [7]

V roce 1969 grantová agentura ministerstva obrany USA ARPA (*Advanced Research Projects Agency*) vyvíjí vlastní experimentální síť s využitím přepojování paketů. Síť je po této agentuře pojmenována jako ARPANET, nic na tomto názvu nezměnilo ani pozdější přejmenování agentury na DARPA (*Defense Advanced Research Projects Agency*). Hlavním úkolem ARPANETu bylo ověření funkčnosti techniky přepojování paketů. Dalším úkolem této sítě bylo umožnění přístupu výzkumným pracovníkům k superpočítačům tehdejší doby, které byly umístěny na významných univerzitách USA. V první fázi měl ARPANET čtyři uzly, které byly umístěny na univerzitách UCLA (*University of California Los Angeles*), UCSB (*University of California Santa Barbara*), dále pak na univerzitě v Utahu a Stanfordu (*Stanford Research Institute – SRI*). Na každé z těchto univerzit byl umístěn univerzální počítač Honeywell DDP516, který sloužil jako IMP (*Interface Message Processor*). Pro přenos paketů mezi uzly se využíval protokol NCP (*Network Control Protokol*). [7] [8] V dalších letech se ARPANET rozrůstal a v roce 1972 měl již 37 uzlů. O rok později byly zapojeny první zahraniční uzly, a to ve Velké Británii a Norsku. Původní záměr na využití ARPANETu, tedy dálkový přístup k superpočítačům a práce na nich, byl uživateli přehlížen a namísto toho, uživatelé začali tuto síť využívat především pro vzájemnou komunikaci pomocí elektronické pošty a elektronických konferencí. [6] [7] ARPANET byl tedy hlavně využit pro vzdálenou spolupráci na projektech a předávání si nabytých zkušeností.

V roce 1973 byly v rámci síťových konferencí, pořádaných skrze ARPANET, položeny základy novému síťovému protokolu TCP. Tvůrci tento protokol ve svém počátku koncipovali jako tzv. spolehlivý protokol. Základní myšlenka byla v potvrzování přijatých paketů příjemcem, tudíž odesílatel věděl, které pakety byly doručeny a které je třeba odeslat znovu. V průběhu vývoje tohoto protokolu došli tvůrci k závěru, že ne vždy je třeba bezchybný přenos dat. Existují totiž i aplikace, kterým nevadí určitým způsobem poškozená data (*např. přenos lidského hlasu*). Původní protokol TCP byl tedy rozdělen na dva nové protokoly, a to na protokol IP (*Internet Protocol*) starající se hlavně o vlastní přenos bez ohledu na spolehlivost. Druhému protokolu bylo zanecháno pojmenování TCP. Tento nový protokol využívá přenosové služby protokolu IP, a navíc k nim zajišťuje spolehlivost. Dále byl vytvořen protokol UDP (*User Datagram Protocol*) pro aplikace upřednostňující rychlost přísunu dat před jejich spolehlivostí. UDP využívá přenosových služeb protokolu IP stejně jako TCP, ale již nezajišťuje spolehlivost přenesených dat. [6] [7] Dnešní podobu dostaly tyto protokoly v roce 1979.

V průběhu sedmdesátých let vznikají další sítě založené na principu přepojování paketů. Tyto sítě se postupně připojují k ARPANETu a ten se na počátku osmdesátých let stává páteřní sítí. V roce 1980 se protokol TCP/IP stává preferovaným protokolem v síti ARPANET. O dva roky později ministerstvo obrany USA rozhoduje o povinném přechodu na tento protokol pro všechny připojené počítače do sítě ARPANET. Dnem 1.1.1983 je ARPANET neprůchozí pro pakety využívající protokol NCP. V tomto roce také dochází ke vzniku čistě armádní sítě MILNET, která vznikla odtržením těch částí sítě ARPANET, které měly cokoli společného s armádou a ARPANET slouží čistě pro civilní účely. [7] Tyto dvě sítě však zůstávají propojené.

Jednou z nejdůležitějších sítí připojených k ARPANETu byl NSFNET (*National Science Foundation Network*), který byl vytvořen NSF (*National Science Foundation*) v roce 1986. Jeho počátky sahají na přelom sedmdesátých a osmdesátých let, kdy většina amerických univerzit neprováděla výzkum pro ministerstvo obrany, a tudíž nemohla být přímo připojena k ARPANETu. Proto v roce 1980 byla za podpory NSF vytvořena síť CSNET (*Computer Science Network*), jejímž úkolem bylo poskytovat síťové služby, včetně elektronické pošty a připojení k ARPANETu, výzkumným skupinám v oblasti počítačové vědy na univerzitách, v průmyslu a státní správě. [9] CSNET propojil v roce 1981 první tři instituce, a to University of Delaware, Princeton University a Purdue University. V následujícím roce CSNET propojoval již 24 institucí a v roce 1984 vzrostl počet připojených institucí na 84. V únoru roku 1984 byl připojen první mezinárodní uzel, a to v Izraeli. Posléze následovaly uzly v Koreji, Austrálii, Kanadě, Francii, Německu a Japonsku. Koncem roku 1985 počet připojených institucí čítal 180. [10] [11] CSNET zásadním způsobem demonstroval možnosti počítačových sítí a pomohl vyvolat poptávku po robustní celostátní síti. Na tuto poptávku NSF zareagovalo vytvořením své vlastní sítě NFSNET.

Při svém vzniku byl NSFNET vytvořen propojením pěti superpočítačových center (*San Diego Supercomputer Center, National Center for Supercomputing Applications, Cornell Theory Center, Pittsburgh Supercomputing Center, John von Neumann Supercomputer Center*) společně s NCAR (*National Center for Atmospheric Research*). Toto páteřní spojení bylo realizováno linkou o rychlosti 56kbit/s. [7] Na tuto páteřní síť se dále připojovaly stávající regionální sítě a místní akademické sítě. NSF se rozhodlo po vzoru CSNETu neomezit NSFNET pouze na výzkumné pracovníky, ale otevřít ji všem akademickým uživatelům. Důsledkem byl obrovský zájem o připojení do této sítě. Tímto se „zrodil“ moderní internet. V prvním roce provozu byl zájem tak vysoký, že rychlost 56kbit/s páteřní sítě byla

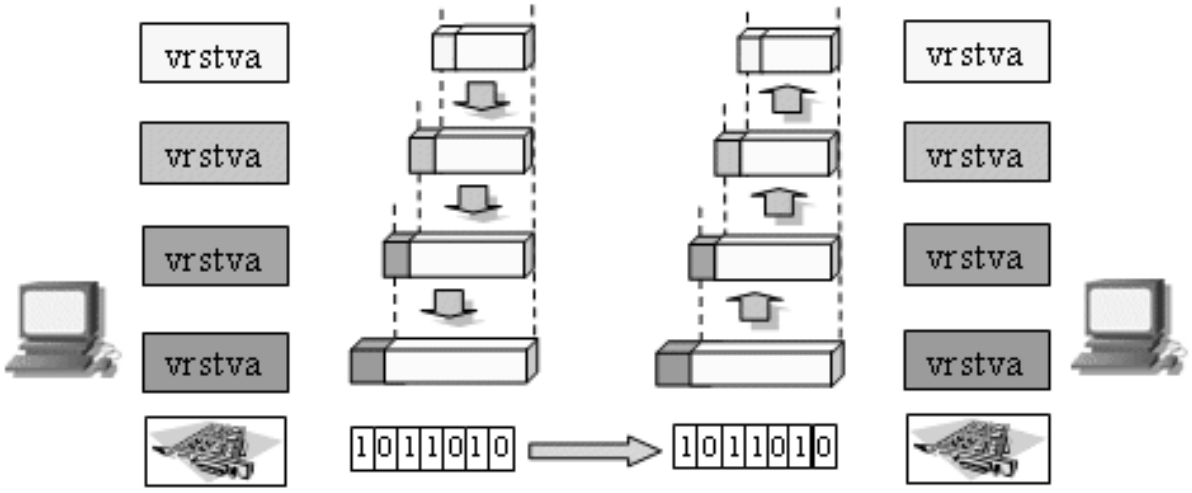
nedostačující. Proto NSF v roce 1987 vyhlásila veřejnou soutěž o návrh upgradu pro NSFNET. Tuto soutěž se svým návrhem vyhrálo konsorcium IBM, MCI a MERIT Network (*Michigan Educational Research Information Triad*), které rychlost zvýšilo na T1 (*1,5 Mbit/s*). Tento upgrade však znamenal i další zvýšení využívání této sítě, které rostlo každý měsíc o 10 %. MERIT Network provedl další upgrade v roce 1991 a to na T3 (*45Mbit/s*). Existence NSFNETu a vytvoření FIX (*Federal Internet Exchanges*) vedlo v roce 1990 k ukončení provozu ARPANETu a ke kompletnímu převzetí jeho úlohy NSFNETem. [12] [13] [14] [15]

V devadesátých letech došlo k privatizaci dosavadního internetu a páteřní síť NSFNET byla vyřazena z provozu 30. dubna 1995.

2 Modely a architektura počítačových sítí

Na úvod této kapitoly je třeba vysvětlit rozdíl mezi modelem a architekturou. *„Architektura není popisem konkrétního systému nebo sítě, ale naopak, určitý systém (např. síť) je vystavěn, provozován a udržován podle jisté architektury. Ze zákonitostí architektury lze vybudovat model, podle něhož se konkrétní systémy mohou budovat.“* [16, s. 39]

Z důvodu velké složitosti síťové komunikace jako celku, se k této problematice přistupuje skrze dekompozici. To znamená, že se celý problém komunikace rozdělí na méně složité problémy a ty se poté řeší jako samostatný celek. V případě počítačových sítí se tento problém rozdělil tzv. „horizontálním řezem“, což mělo za následek vznik hierarchicky uspořádaných vrstev s vlastními specifickými úkoly. Počet těchto vrstev je závislí na konkrétním typu architektury. [17] Výhodou těchto vrstev je jejich interoperabilita, jinak řečeno konkrétní vrstva daného uzlu využívá služeb, které poskytuje vrstva bezprostředně nižší a sama poskytuje služby vrstvě bezprostředně vyšší. Tento typ komunikace je označován jako vertikální komunikace neboli služby. Dále tuto konkrétní vrstvu lze vyměnit, aniž by bylo třeba zasahovat do vrstev přímo sousedících. Druhým typem komunikace mezi vrstvami je komunikace horizontální. Jedná se o komunikaci mezi vrstvami na stejné úrovni dvou navzájem komunikujících uzlů. Pro tuto komunikaci se využívá PDU (*Protocol Data Unit*). Při odesílání se PDU předává vrstvami směrem od nejvyšší k nejnižší a jednotlivé vrstvy, kterými prochází, přidávají k PDU své vlastní informace. Těmto informacím rozumí jenom vrstva na stejné úrovni druhého uzlu a ostatní vrstvy ji berou jenom jako data. Tomuto způsobu komunikace se říká protokol. [18]



Obrázek 1 – Horizontální komunikace mezi vrstvami [37]

2.1 Architektura počítačových sítí

Historie síťových architektur sahá až na samý počátek vzniku sítí samotných. Problém byl však v tom, že architektury pro tyto sítě byly proprietární, jinak řečeno specifické pro konkrétního výrobce, a neexistovala tu vzájemná interoperabilita. Ve chvíli, kdy se jednotlivé sítě s různými architekturami začaly propojovat, vyvstal požadavek na ne-proprietární architekturu, která by byla dostatečně otevřená a umožňovala dostatečnou kompatibilitu.

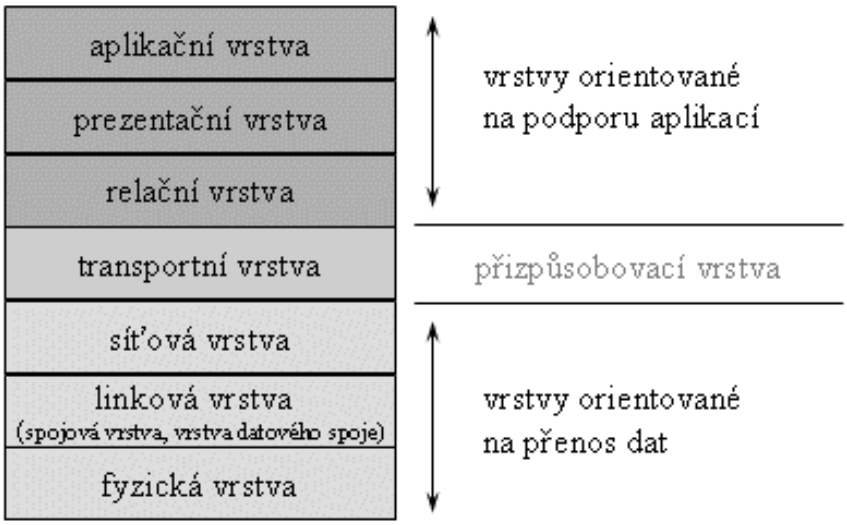
Takovouto architekturu dobrovolně vybudovala organizace ISO (*International Organization for Standardization*). [17] Původní záměr této organizace byl však trochu jiný. Chtěla vytvořit standard pro fungování otevřených systémů OSA (*Open System Architecture*). Tento standard měl být použitelný nejenom pro sítě a uzly v nich obsažených, ale i pro fungování všech počítačů. Záměr byl však na tehdejší dobu, a troufám si říct i na dnešní, příliš ambiciózní. Proto se organizace ISO rozhodla při vývoji standardu soustředit pouze na komunikaci těchto komponent a název standardu byl upraven na OSIA (*Open System Interconnection Architecture*). Nakonec ISO musela ze svého záměru slevit ještě jednou, a to z důvodu neochoty použít již některá standardizovaná řešení. [19] Vytvořený standard byl pojmenován jako RM OSI (*Reference Model for Open System Interconnection*), který definuje počet vrstev a jejich jednotlivé úkoly, ale bez potřebných protokolů. Ty měli být postupně doplňovány.

ISO do tohoto projektu investovalo velké úsilí a nemalé prostředky. Očekávalo, že tento standard bude zaveden všemi jeho členskými státy. To se však nestalo. Celá koncepce standardu byla totiž vyvíjena čistě od stolu. Shromáždilo se určité množství požadavků, které byly vydány jako standard. Poté se zjišťovalo, zda jsou tyto požadavky v praxi vůbec realizovatelné, popřípadě nákladnost těchto realizací. Druhým důvodem pro nezavedení do praxe, bylo to, že trh nedisponoval produkty postavenými na tomto standardu. Tímto se uzavřela kapitola RM ISO OSI jako architektury a „vládnoucí“ architekturou, až do dnešní doby, se stala rodina protokolů TCP/IP. [17] [19]

2.2 Referenční model ISO OSI

RM ISO OSI se v dnešní době využívá hlavně na poli teorie počítačových sítí, a to především jeho model vrstev. Tento vrstvový model se v první řadě využívá k vysvětlení základních principů komunikace v počítačových sítích.

Vrstvový model RM ISO OSI je tvořen sedmi vrstvami, které jsou rozděleny do tří skupin. Vrstvy 1-3 tvoří skupinu nižších vrstev. Tato skupina je orientována na spojení a přenos dat. Vrstvy 5-7 tvoří skupinu vyšších vrstev. Účelem této skupiny je zpracování dat pro potřeby aplikací. Poslední skupina je jednočlenná, obsahující pouze vrstvu číslo 4. Tato skupina přizpůsobuje data pro potřeby předchozích skupin. Z tohoto důvodu nese název přizpůsobovací. [20, s. 33]



Obrázek 2 – Sedm vrstev RM ISO OSI [38]

Popis a funkce jednotlivých vrstev jsou dále postupně popsány směrem od nejnižší po nejvyšší.

2.2.1 Fyzická vrstva

Základní funkcí této vrstvy je kódování dat získaných od linkové vrstvy, která jsou vyjádřena binárním kódem (*soustava jedniček a nul*), na signál odpovídající přenosovému médiu (*impulsy světla, změna napětí, modulací*) a naopak. [21, s. 136] Na této vrstvě se dále řeší druhy přenosu (*synchronní, asynchronní, sériový, paralelní*) a přenosová kapacita. Existují tu i určité standardy (*ISO*[1]*, IEEE*[2]*, ANSI*[3]*, FCC*[4]*, EIA/TIA*[5]) pro zajištění kompatibility hardwaru od různých výrobců, jako třeba druhy koncovek kabelů, fyzické vlastnosti přenosových médií. Tato vrstva žádným způsobem nerozlišuje přenášená data, jinak řečeno, ke všem datům se chová stejným způsobem. [17] [21, s. 137]

[1] International Organization for Standardization
[2] Institute of Electrical and Electronics Engineers
[3] American National Standards Institute
[4] Federal Communication Commission
[5] Electronics Industry Alliance/Telecommunications Industry Association

2.2.2 Linková vrstva

Pro tuto vrstvu se často užívá i označení spojová vrstva. Jejím hlavním úkolem je příprava (*obalení*) odesílaných dat pro přenos na fyzické médium. To spočívá v přidání speciálních skupin jedniček a nul k odesílaným datům. Tímto vznikne tzv. rámec (*z angl. frame*). Tyto rámce dokáže přenášet však pouze k přímo připojeným uzlům. Struktura rámce je hlavička, data a patička. Hlavička rámce obsahuje informace o jeho začátku, fyzickou adresu příjemce (*MAC adresa*) a další v závislosti na použitém protokolu. V patičce jsou informace o konci rámce a informace o kontrole chyb v něm. Z důvodu vzniku sítí LAN, které pro komunikaci využívají sdílení přenosového média došlo k rozdělení této vrstvy na dvě podvrstvy. Vyšší podvrstva řízení logických spojů LLC (*Logical Link Control*) obstarává původní funkce a nižší podvrstva řízení přístupu k médiu MAC (*Media Access Control*) zajišťuje přístup na sdílenému médiu. [17] [21, s. 122-126] [22, s. 4]

Pro řízení přístupu na sdílené médium existují dvě základní metody. Deterministická a nedeterministická. Princip deterministické metody je založen na střídavém vysílání jednotlivých uzlů. Pokud uzel nemá co vysílat, vysílá další v pořadí, ale musí počkat na doručení předešlých dat příjemci. Nedeterministická spočívá v pokusech o vysílání uzlů, které aktuálně potřebují něco vysílat. Využívá se tu metody CSMA (*Carrier Sense Multiple Access*), která spočívá v tom, že pokud uzel chce vysílat, naslouchá, zdali je přenosové médium volné, pokud není, čeká určitý časový úsek a pokus opakuje. [21, s. 126-127]

2.2.3 Síťová vrstva

Primárním úkolem této vrstvy je zprostředkování komunikace a přenos dat (*paketů*), mezi uzly, které mezi sebou nemají přímé spojení. Spojení těchto uzlů je tedy realizováno přes určitý počet jiných uzlů, tzv. mezilehlých uzlů. Aby tato vrstva byla schopná realizovat takovýto druh spojení, používá za tímto účelem čtyři základní procesy. Těmito procesy jsou adresování (*angl. addressing*), zapouzdření do paketu (*angl. encapsulation*), směrování (*angl. routing*) a posledním procesem je rozbalení (*angl. decapsulation*). [17] [21, s. 63] [22, s. 4-5] Adresace a směrování jsou rozebírány podrobněji v dalších kapitolách této práce.

Proces adresace spočívá v přidělení unikátní síťové adresy IP (*logické adresy*), bez ohledu na použitý protokol, každému uzlu v síti. Tato síťová adresa je dále využita v dalším procesu, a to v zapouzdření. Proces zapouzdření přidává k datům získaných z transportní vrstvy tzv. hlavičku, která obsahuje tuto IP adresu, a to jak IP adresu příjemce, tak i odesílatele. Tento proces však platí, pokud jsou oba uzly ve stejné síti. Pokud je odesílatel v jiné síti než příjemce,

musí se využít třetí proces této vrstvy a tím je směrování. Pro proces směrování jsou důležité routery, což jsou síťové prvky, které propojují jednotlivé sítě. V routerech jsou obsaženy tzv. routovací tabulky. Na základě těchto tabulek a IP adresy příjemce, která je obsažena v příchozím paketu, rozhodují o tom, jakým směrem došlý paket přepošlou. [21, s. 63] [19] Tímto způsobem cestuje paket skrze sítě, do doby, než dorazí k příjemci. Po úspěšném přenosu paketu k příjemci, přichází na řadu čtvrtý proces, rozbalení paketu. Na síťové vrstvě příjemce dojde k rozbalení paketu, čímž se z něj odstraní hlavička a zbylá data jsou předána transportní vrstvě příjemce.

Ve vrstvě se využívá několik protokolů, přičemž za zmínku stojí nejrozšířenější protokol IP (*Internet Protocol*) ve verzi IPv4 a IPv6, dále pak protokol ICMP (*Internet Control Message Protocol*). Dříve to byly také protokoly IPX (*Internetwork Packet Exchange*) od Novell NetWare a AppleTalk od Apple, který se využíval pro počítače Macintosh. [21, s. 63] [22, s. 5].

2.2.4 Transportní vrstva

Pro tuto vrstvu jsou charakteristické tři základními vlastnosti. Těmito vlastnostmi jsou segmentace dat, rozlišování příjemců a odesílatelů v rámci jednoho uzlu a spolehlivost přenosu dat. Dále tato vrstva tvoří pomyslnou hranici mezi vrstvami zabývající se protokoly přenosu dat a vrstvami zabývajíce se protokoly podporující aplikace. Komunikace probíhající na této vrstvě je označována jako „end – to – end“ komunikace, protože na rozdíl od předchozích vrstev neprobíhá s přímo sousedícími uzly, ale až s koncovými. To znamená, že komunikuje jenom odesílatel s příjemcem. [17] [21, s. 54]

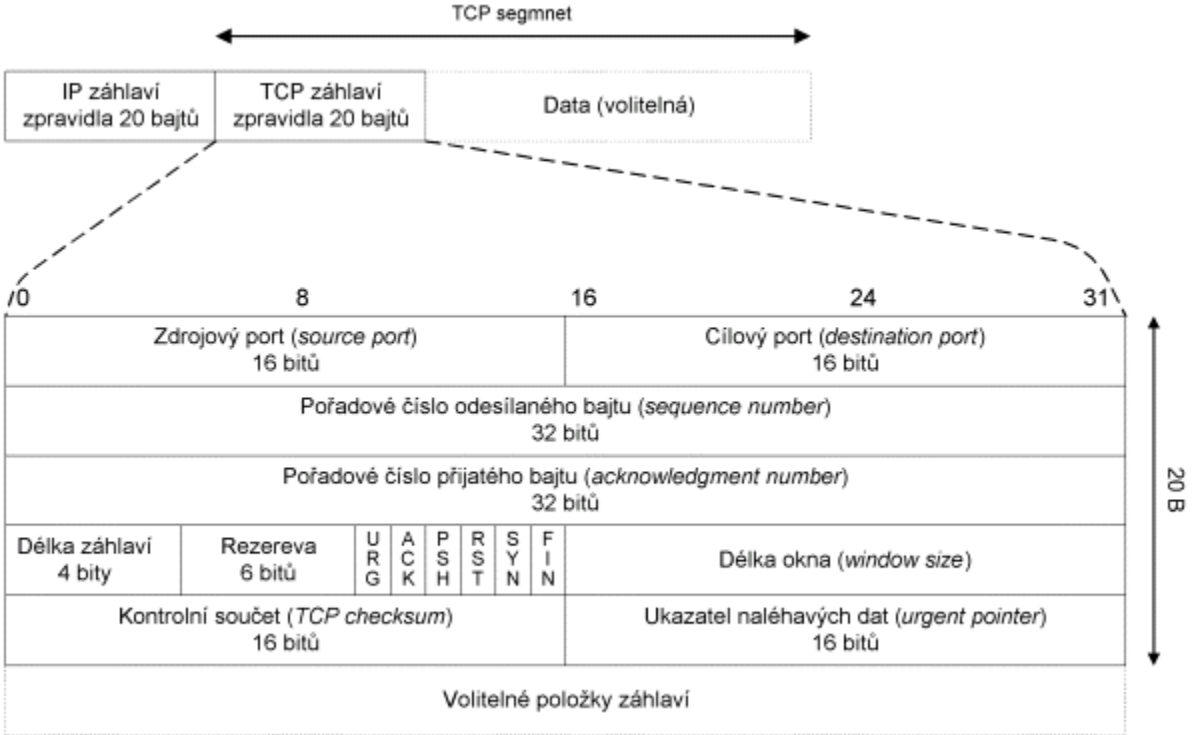
Segmentace dat je označení pro proces, kdy jsou příchozí data z vyšších vrstev dělena na menší části, tzv. segmenty. Po přijetí příjemcem jsou tyto segmenty opět složeny do jednoho celku. Toto složení probíhá na základě čísel, která jsou jednotlivým segmentům přiřazena při jejich vzniku. Chybějící nebo poškozený segment řeší funkce spolehlivost přenosu. Účelem segmentace je možnost přenosu dat více aplikací současně. Pokud by se data jedné aplikace posílala v celku, potom by další aplikace, která by chtěla vysílat, musela počkat až budou odeslána data první aplikace. [21, s. 54]

Na této vrstvě se již rozlišují jednotliví odesílatelé a příjemci (*aplikace*) dat v rámci daného uzlu. Pro to, aby bylo možné od sebe jednotlivé odesílatele a příjemce rozlišit jsou zde definovány body SAP (*Service Access Point*), neboli porty. [17] Tyto porty jsou označeny šestnáctibytovým číslem. Číslo odchozího portu í cílového je obsaženo v paketu společně

s ostatními daty. Data jsou po přijetí přes tyto porty převzata příslušnými příjemci, či při odesílání odevzdána příslušnými odesílateli. [21, s. 61]

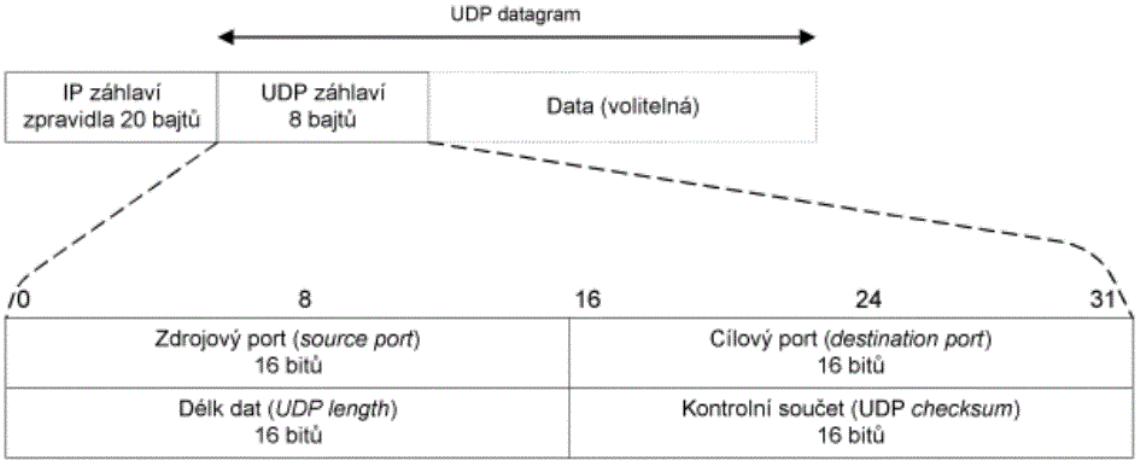
V rámci přenosu jednotlivých segmentů, může dojít k situaci, kdy segment nedorazí do cíle vůbec, nebo dorazí, ale poškozený. Z tohoto důvodu na této vrstvě existuje služba spolehlivosti přenosu dat. Tato služba pro své účely využívá dva základní protokoly, a to protokol TCP (*Transmission Control Protocol*) a UDP (*User Datagram Protocol*). Tyto protokoly jsou použity na základě požadavků jednotlivých aplikací.

TCP je spojově orientovaný protokol. To znamená, že pro dvě aplikace vytvoří spojení tzv. virtuální okruh. Tento protokol je použit, pokud aplikace požaduje kompletní a bezchybný přenos dat. Princip tohoto protokolu spočívá v potvrzování přijatých segmentů příjemcem. Odesílatel odešle segment a čeká určitý čas na potvrzení jeho přijetí příjemcem. Nedojde-li k potvrzení přijetí segmentu, považuje tento segment za ztracený a opětovně ho odesílá. Správné pořadí segmentů je určováno pomocí čísel, které jsou jednotlivým segmentům přiřazena při jejich vzniku. To, zda je segment poškozen či nikoli je ověřeno výpočtem kontrolního součtu. Tato hodnota je uložena do odesílaného segmentu. Po přijetí se výpočet provede znovu a výsledek je porovnám se záznamem v segmentu. [21, s. 56-59] [22, s. 40] [23, s. 217] Aplikace, které využívají tento protokol jsou např. e-mail, přenos souborů, www, ….



Obrázek 3 – Hlavička protokolu TCP [39]

Protokol UDP je na rozdíl od TCP nespojově orientovaný protokol. Je to jakási jednodušší verze protokolu TCP. V tomto protokolu je segment nahrazen pojmem datagram. Tyto datagramy při svém vzniku nejsou číslovány. Protokol nezasílá potvrzení o přijetí datagramů a ani nekontroluje to, zda jsou poškozené či nikoli. Nestará se ani o správné řazení datagramů. Datagramy jsou u příjemce řazeny v pořadí, v jakém přišli. Správné řazení datagramů si musí aplikace ohlídat sama, pokud to vyžaduje. Mezi aplikace využívající tento protokol se řadí DNS (*Domain Name System*), VoIP[6] (*Voice over Internet Protocol*), streamování videa. [21, s. 60] [22, s. 39-40]



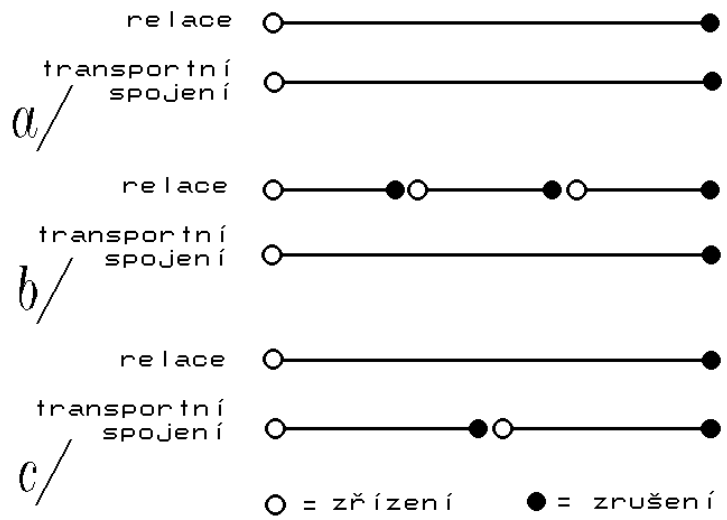
Obrázek 4 – Hlavička protokolu UDP [40]

2.2.5 Relační vrstva

„Analogii práce relační vrstvy bychom mohli najít v práci manuálních telefonních ústředen minulosti: Operátorka na základě usneseného požadavku spojila volajícího s požadovaným volaným, monitorovala hovor a po jeho dokončení spojení ukončila.“ [16, s. 54] Základem této vrstvy je relace. Dle výše uvedené citace můžeme relaci definovat jako spojení mezi dvěma aplikacemi. Vrstva má za úkol tyto relace vytvářet, spravovat a ukončovat. Každá relace je realizována pomocí jednoho transportního spojení (*spojení na bezprostředně nižší vrstvě*). Mohou však nastat i další dva případy, a to v důsledku různých délek trvání spojení. První případ, kdy v průběhu jednoho transportního spojení je realizováno více po sobě

[6] Přenos digitalizovaného hlasu prostřednictvím počítačové sítě

následujících relací. Druhý je přesně opačný, více po sobě následujících transportních spojení je využito jednou relací. [16, s. 54] [24]



Obrázek 5 – Vztah relace a transportního spojení [41]

Další funkcí této vrstvy je synchronizace. Účelem synchronizace je možnost opětovného vyžádání již přijatých dat, která byla z důvodu poruchy zařízení využívající tato data ztracena. Data si však nepamatuje vrstva samotná, nýbrž jejich odesílatel, který tuto vrstvu využívá. Pro tyto účely může vrstva do odesílaných dat vkládá dva druhy synchronizačních bodů. Prvním z těchto bodů je vedlejší synchronizační bod, za který se lze vracet. Druhým je hlavní synchronizační bod, za který se již vrátit nelze. [24] Stručně řečeno, odesílatel si musí pamatovat jenom data od posledního hlavního a následujících vedlejších synchronizačních bodů.

2.2.6 Prezentační vrstva

Jelikož počítače používají různé vnitřní standardy interpretací a kódování dat, je zapotřebí pro jejich vzájemnou komunikaci zajištění konverze těchto přenášených dat. O tuto konverzi se stará právě tato vrstva, přesněji řečeno zajišťuje zachování významu dat a jejich prezentaci pro účely aplikační vrstvy. V této vrstvě, jako v jediné, může dojít k pozměnění přenášených dat. Za tímto účelem je v této vrstvě vyžíváno komprese a dekomprese dat, jejich kódování, šifrování a dešifrování. [16, s. 53] [17]

Vrstva data konvertuje hned dvakrát. Poprvé jsou konvertována při odesílání z formátu, se kterým pracuje odesílatel na přenosový formát. Podruhé jsou konvertována z přenosového formátu na formát, se kterým pracuje příjemce. Pro tento účel byl vyvinut jazyk ANS.1 (*Abstract Syntax Notation*), který zajišťuje zakódování dat do tzv. přenosové syntaxe a jejich zpětné rozkódování. V této syntaxi je popsán charakter přenášených dat, a tudíž po rozkódování

prezentační vrstvou příjemce, jsou data prezentována aplikační vrstvě ve stejném významu, ve kterém byla odeslána. [25] [26, s. 52]

2.2.7 Aplikační vrstva

Tato vrstva je sedmou, tudíž poslední a nejvyšší vrstvou RM ISO OSI. Dle názvu by se dalo očekávat, že se v této vrstvě budou nacházet a provozovat samotné aplikace, opak je pravdou. Původní návrh RM ISO OSI sice počítal s tím, že aplikace budou součástí této vrstvy, ale postupem času se tato varianta modifikovala a v této vrstvě zůstaly pouze síťové služby, které jednotlivé aplikace využívají. Jsou jimi tiskové služby, dále souborové, databázové, aplikační a služby zasílání zpráv. Tyto síťové služby jsou tvořeny prvky ASE (*Application Service Elements*), které jsou dvojího typu. Prvním typem jsou prvky CASE (*Common Application Service Elements*) zajišťující síťové služby pro potřeby různých aplikací. Druhým typem jsou prvky SASE (*Specific Application Service Elements*), které zajišťují síťové služby pro konkrétní druh aplikací. S těmito prvky dále souvisí i protokoly používané na této vrstvě. Těmi jsou např. DNS, SMTP, FTP, TELNET, DHCP [26, s. 51-52] [27]

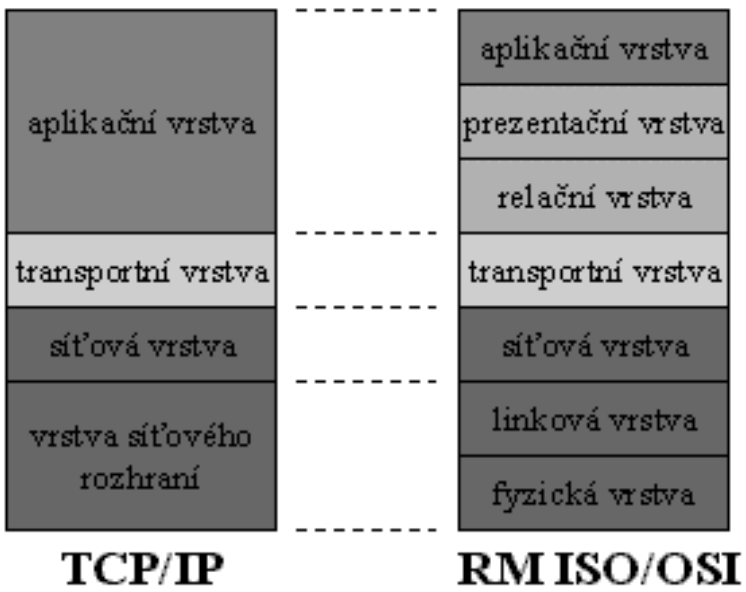
Hlavním účelem této vrstvy je tedy umožnit aplikacím přístup k síťové komunikaci a umožnit jejich vzájemnou spolupráci.

2.3 TCP IP

Historie vzniku této architektury sahá do první poloviny sedmdesátých let minulého století a je úzce spjata se sítí ARPANET, pro kterou byla tato rodina protokolů vytvořena jako nástupce protokolu NCP. Název tato architektura získala po dvou jejích nejznámějších protokolech, kterými jsou protokoly TCP (*Transmission Control Protocol*) a IP (*Internet Protocol*). Protokolů tato architektura obsahuje samozřejmě mnohem více. Základem této architektury jsou čtyři vrstvy a dále úkoly, které tyto vrstvy mají plnit. Pro plnění těchto úkolů jsou využívány již zmíněné protokoly, které tato architektura obsahuje.

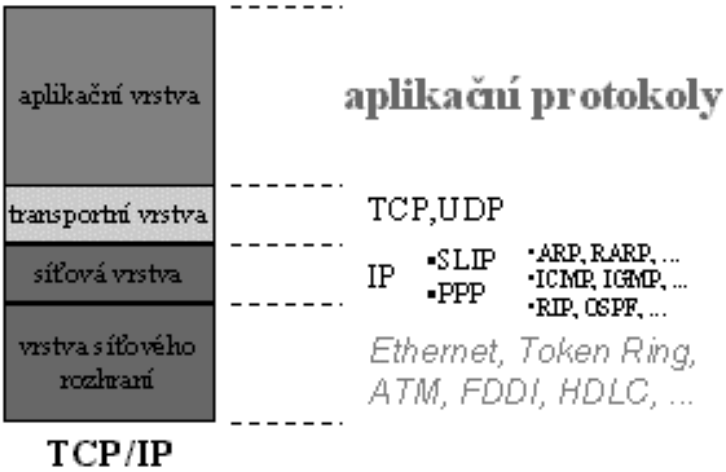
Pro definici protokolů a standardů této architektury slouží tzv. dokumenty RFC (*Request For Comments*). [20, s. 34] Tyto RFC stojí za samotným vznikem protokolů této vrstvy. Každý dokument RFC má své vlastní pořadové číslo a je veřejně přístupný, nejčastěji na internetu. Tyto dokumenty se nemění, jejich aktualizace probíhá vydáním nového dokumentu RFC s novým pořadovým číslem. V dnešní době existuje přes 5000 těchto dokumentů. Nutno podotknout, že ne všechny dokumenty RFC se týkají architektury TCP IP. Část těchto dokumentů se zabývá standardy a popisem chování samotného internetu.

Důvodem, proč má tato architektura čtyři vrstvy oproti sedmi RM ISO OSI, není v tom, že jsou od sebe tolik odlišné, ale spíše v přístupu jejich tvůrců. Postup a řešení u architektury TCP IP byl zcela odlišný od té u RM ISO OSI. Tvůrci architektury TCP IP se vydali cestou postupného zdokonalování jednotlivých řešení a za standard bylo vydáno teprve řešení, které bylo nejdříve odzkoušeno a ověřena schopnost implementace v reálném světě. [28]



Obrázek 6 – Srovnání vrstev RM ISO OSI a TCP IP [42]

Jednotlivé funkce a protokoly vrstev architektury TCP IP jsou dále popsány od té nejnižší až po nejvyšší. Nejedná se o detailní popis jako v případě RM ISO OSI, ale o upřesnění těchto funkcí a představení protokolů charakteristických pro tyto vrstvy. Důvodem pro méně detailní popis vrstev architektury TCP IP je velká shoda, nebo dokonce totožnost jako v případě RM ISO OSI. Podrobnější popis protokolů a vrstev architektury TCP IP se nachází v RFC. Seznam doporučených RFC k seznámení viz [16, s. 243-244].



Obrázek 7 – Protokoly a vrstvy TCP IP [43]

2.3.1 Vrstva síťového rozhraní

Vrstva síťového rozhraní (*Network Interface Layer*) je nejnižší vrstvou této architektury. Pro velmi časté použití přenosového prostředí Ethernet se tato vrstva někdy označuje i jako Ethernetová vrstva (*Ethernet Layer*). [29] Její analogií v RM ISO OSI jsou vrstvy Fyzická a Linková. Tato vrstva se stará o kompletní zabezpečení přenosové cesty, vysílání a příjem jednotlivých datových paketů. Pro tuto architekturu není tato vrstva podrobněji definována z důvodu možného použití více druhů různých přenosových prostředí. Může se jednat například o Ethernet (*IEEE 802.3*), FDDI/ANSI, Token Ring (*IEEE 802.5*), WLAN (*IEEE 802.11, 802.15, 802.16*), Fiber Chanel/ANSI. [16, s. 77-78, 245-246] [19]

2.3.2 Síťová vrstva

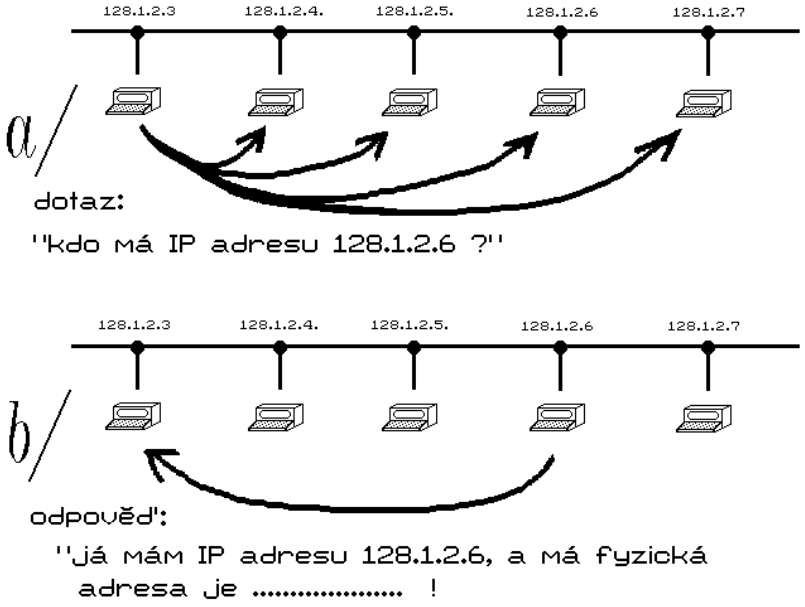
Síťová vrstva (*Internet Layer*), označována také jako IP vrstva (*IP Layer*) dle protokolu IP, pomocí kterého je realizována, je druhou vrstvou architektury TCP IP. Protokol IP má i vliv na typ poskytované síťové služby. Tento protokol funguje nespolehlivě, tudíž poskytuje síťovou službu bez spojení a jako základ slouží datagram. Vrstva odpovídá Síťové vrstvě v RM ISO OSI a z tohoto důvodu i její funkce je obdobná. Pro poskytování svých služeb využívá tato vrstva několik typů protokolů. Prvním, již zmíněným, je protokol IP (*ve verzi 4 a 6*), dále pak protokol mapování adres ARP (*Address Resolution Protocol*), protokol reversního mapování adres RARP (*Reverse Address Resolution Protocol*), protokol řídících hlášení ICMP (*Internet Control Message Protocol*), protokol správy skupin stanic (*Internet Group Management Protocol*) a směrovací protokoly RIP (*Routing Information Protocol*), OSPF (*Open Shortest Path First*) a IGRP (*Interior Gateway Routing Protocol*). [16, s. 246-247] Jednotlivé protokoly jsou následně přiblíženy, mimo protokolů IP a směrování, pro které jsou v této práci vyhrazeny samotné kapitoly.

Pro potřeby komunikace mezi dvěma zařízeními v síti slouží IP datagram, který v sobě obsahuje IP adresu jak odesílatele, tak i IP adresu příjemce. Tento IP datagram je dále zabalen do datagramu přenosového prostředí, v případě Ethernetu jde o ethernet datagram. Hlavička tohoto ethernet datagramu obsahuje fyzickou (*MAC*) adresu odesílatele i příjemce. Proto je pro potřebu komunikace mezi dvěma zařízeními tyto adresy, IP i MAC, znát. [23, s. 153]

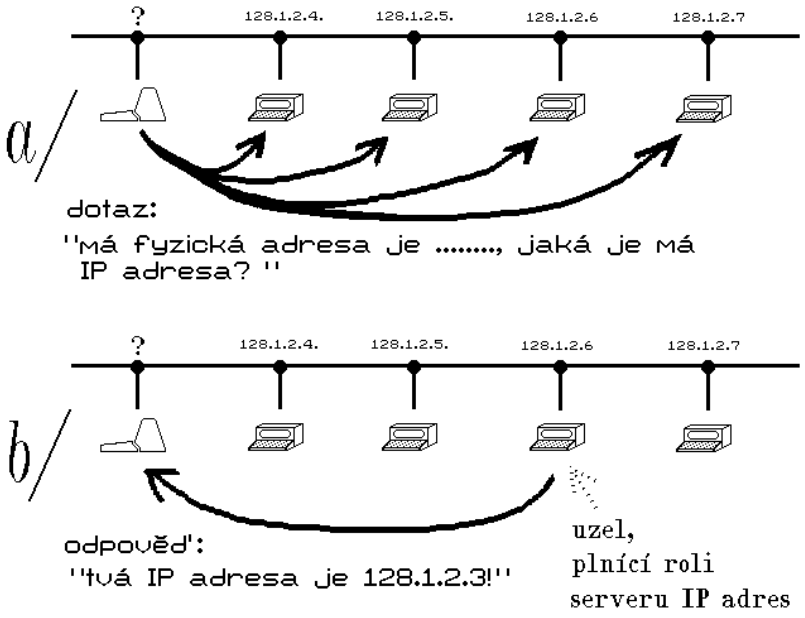
Mohou nastat případy, kdy odesílatel ve své ARP cache nenajde MAC adresu příjemce, a tudíž zná pouze jeho IP adresu. Pro tyto případy slouží v architektuře TCP IP protokol ARP, který je schopen MAC adresu v síti zjistit pomocí vyslání všesměrové zprávy tzv broadcast.

Tuto zprávu dostanou všechna zařízení v síti, ale odpoví pouze zařízení, které má hledanou MAC adresu. Ta je zaslána v odpovědi odesílateli broadcastu. [16, s. 260-262] [23, s. 153-157]

Protokol RARP je využíván hlavně u zařízení, která nejsou schopna uložit, nebo pamatovat si svoji IP adresu. Takové zařízení po svém spuštění potřebuje zjistit svoji IP adresu. Vyšle do sítě broadcast se svojí MAC adresou, s dotazem na svoji IP adresu. Dostane odpověď od serveru, který má na starosti přidělování IP adres. Tento protokol byl v praxi postupně nahrazen protokolem DHCP (*Dynamic Host Configuration Protocol*), který jednotlivým zařízením v síti dynamicky přiděluje IP adresy, masky, brány. [16, s. 262] [23, s. 158]



Obrázek 9 – Protokol ARP [44]



Obrázek 8 – Protokol RARP [45]

Dalším protokolem na Síťové vrstvě je protokol ICMP. Tento protokol slouží pro vysílání speciálních zpráv, které se týkají chyb a mimořádných situacích při přenosu jednotlivých datagramů. Existují dva druhy ICMP zpráv, těmi jsou chybové a dotazové zprávy. Patří sem například echo, time exceeded, address mask request, destination unreachable. Všechny typy hlášení protokolu je možné nalézt v RFC 192 a RFC 1256 a RFC 1122. [16, s. 262-264] [22, s. 46] [23, s. 135-141]

2.3.3 Transportní vrstva

Úloha této vrstvy je obdobná jako u RM ISO OSI, tím je zajištění přenos dat mezi koncovými uzly komunikace. Protokoly TCP a UDP, které tuto vrstvu nejvíce specifikují, byly již popsány v RM ISO OSI, viz strana 20 této práce.

2.3.4 Aplikační vrstva

Narozdíl od RM ISO OSI, ve kterém této vrstvě předcházejí vrstvy relační a prezentační zajišťující pro aplikační vrstvu podpůrné služby, v této architektuře tyto vrstvy nenajdeme. Je to způsobeno myšlenkou tvůrců architektury TCP IP, že tyto takzvané podpůrné služby nebudou často potřebné. Z tohoto důvodu není potřeba tyto služby implementovat do samostatných vrstev. Implementaci jednotlivých podpůrných služeb, si musí každá aplikace zajistit samostatně dle vlastní potřeby. [28]

3 Rozdělení sítí a standardy sítí LAN

Počítačové sítě se rozdělují dle různých hledisek. Může se jednat o rozlohu sítě, topologii, metody přístupu, standardu přenosového prostředí, přenosové rychlosti a dle dalších kritérií.

3.1 Rozdělení dle rozlohy sítě

Toto rozdělení počítačových sítí je na základě jejich rozlehlosti neboli velikosti či jejich dosahu. Dle tohoto kritéria se sítě dělí na PAN (*Personal Area Networks*), LAN (*Local Area Networks*), CAN (*Campus Area Networks*), MAN (*Metropolitan Area Networks*), WAN (*Wide Area Networks*), GAN (*Global Area Networks*). Nově se můžeme setkat i se sítěmi NAN (*Neighborhood Area Network*) a CAN (*Community Area Network*).

3.1.1 Sítě PAN

Síť PAN je co do rozsahu nejmenší síť. Tyto sítě nejčastěji představují propojení osobního počítače, notebooku a mobilního telefonu do vzdálenosti několika metrů. Propojení může být realizováno drátovou (*USB*) nebo bezdrátovou (*Wi-Fi, Bluetooth*) technologií. [30] [31]

3.1.2 Sítě LAN

Tento typ je asi nejznámějším a také nejrozšířenějším typem sítí. Jejich rozlehlost se počítá do okruhu několika desítek až stovek metrů. Jsou typické zejména pro domácnosti, malé a střední podniky. Slouží především ke sdílení internetového připojení, síťových disků, tiskáren. Tyto sítě si ve většině případů buduje uživatel sám a na své vlastní náklady. Využívá se zde přenosových technologií Wi-Fi a Ethernet. Přenosové rychlosti se v dnešní době pohybují do 1 Gbit/s. [30] [31]

3.1.3 Sítě CAN

Sítě CAN jsou ve své podstatě sítě MAN, avšak jsou využity pro specifické účely. Propojují rozlehlé části universit, škol, kampusů, fakult, dále se jedná o podnikové sítě velkých firem. Tyto sítě jsou spravovány a vlastněny těmito organizacemi. [30]

3.1.4 Sítě MAN

Toto označení se používá pro typy sítí, které svým rozsahem pokrývají oblasti velikosti měst. Jsou tvořeny propojením několika sítí typu LAN. Jako přenosové médium se v těchto

sítích využívá především optické vlákno nebo přenos pomocí mikrovln. Přenosová rychlost v těchto sítích je v řádu stovek Mbit/s.

3.1.5 Sítě WAN

Tyto sítě jsou charakteristické pro komunikaci na velkou vzdálenost. Jsou velmi rozlehlé a překračují hranice města, okresu, kraje, státu. Realizace těchto sítí bývá přes pronajaté linky, pomocí přepojování okruhů, přepojování paketů a přepojování buněk. Přenosové rychlosti se v tomto typu sítí pohybují v rozmezí od desítek kbit/s do Gbit/s. [31]

Realizace přes pronajaté linky bývá nejdražší, ale také nejbezpečnější. Toto propojení se také označuje jako point-to-point. [30]

Přepojování okruhů funguje na principu telefonní sítě. Tato realizace je nejlevnější. Nutnost sestavení komunikační linky před začátkem vysílání. Není potřeba komunikačního protokolu, protože komunikační linku muže využívat v daný moment jenom jeden odesílatel a jeden příjemce. [30]

V dnešní době nejčastějším způsobe realizace WAN sítí je pomocí přepojování paketů. Komunikační linka je využívána více odesílateli a příjemci, tudíž všichni musí požívat komunikační protokol, který je pro všechny stejný. Rychlost je zde sdílena všemi komunikujícími. [30]

3.1.6 Sítě GAN

Tento druh sítě je tvořen především satelity a bezdrátovými technologiemi. Obecně slouží především pro propojování sítí WAN. Rozsah sítě tohoto typu je v podstatě neomezený. Typickým představitelem je internet. [30] [31]

3.2 Topologie sítí

Dalším kritériem, dle kterého se sítě mohou dělit, je jejich topologie. Topologie popisuje způsob rozmístění jednotlivých prvků sítě. V počítačových sítích se rozlišují dva druhy topologií. Prvním typem je topologie fyzická a druhým typem je topologie logická.

3.2.1 Fyzická topologie

Fyzická topologie popisuje způsob, jakým jsou jednotlivá zařízení v síti mezi sebou propojena. Propojení jednotlivých zařízení je realizováno pomocí koaxiálního kabelu, kroucené dvoulinky, optického kabelu, nebo pomocí bezdrátových technologií jakými jsou rádiový,

mikrovlnný nebo infračervený přenos. Mezi základní fyzické topologie patří sběrnicová topologie, kruhová topologie, topologie hvězdy, stromová a síť se smyčkami.

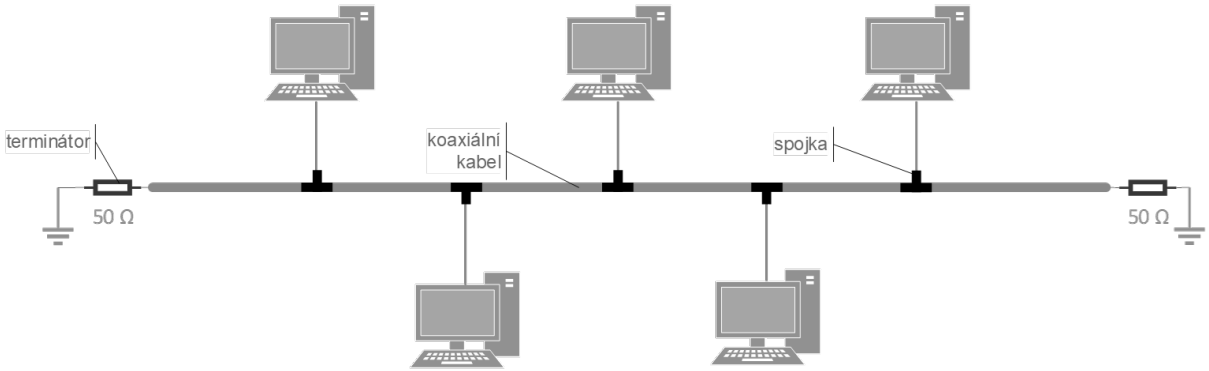
3.2.1.1 Dvoubodové spojení

Dvoubodové spojení neboli také linka, je nejjednodušším typem fyzické topologie. Typickým příkladem této topologie je modemové spojení.

3.2.1.2 Sběrnicová topologie

Sběrnicová topologie (*BUS topology*) je topologií bez centrálního uzlu. Jednotlivé uzly (*stanice*) jsou připojeny ke společnému přenosovému médiu pomocí spojek a odboček. Přenosové médium, kterým je ve většině případů koaxiální kabel, je na obou svých koncích zakončeno tzv terminátory, což jsou odpory o impedanci 50 Ohmů. Zakončení pomocí těchto terminátorů je zde z důvodu, aby na koncích přenosového média nedocházelo ke zpětnému odrazu signálu. Přenos dat je v této topologii realizován pomocí elektrických signálů, a z tohoto důvodu se tento signál šíří v celé délce přenosového média. Teoreticky mají tedy všechny uzly přístup ke všem datům vyslaným do sítě, v praxi se ale dostanou jenom k informaci, která jim je určena pomocí cílové adresy obsažené v přenášených datech. [16, s. 37] [21, s. 133]

Výhody této topologie jsou v její jednoduchosti, snadnému přidání a odebrání uzlu a v malých provozních a pořizovacích nákladech. Hlavní nevýhodou této topologie je v přenosovém médiu. Pokud nastane jakýkoli problém s tímto médiem, může dojít k výpadku celé sítě. Další nevýhodou je možný přenos jen jedné informace.

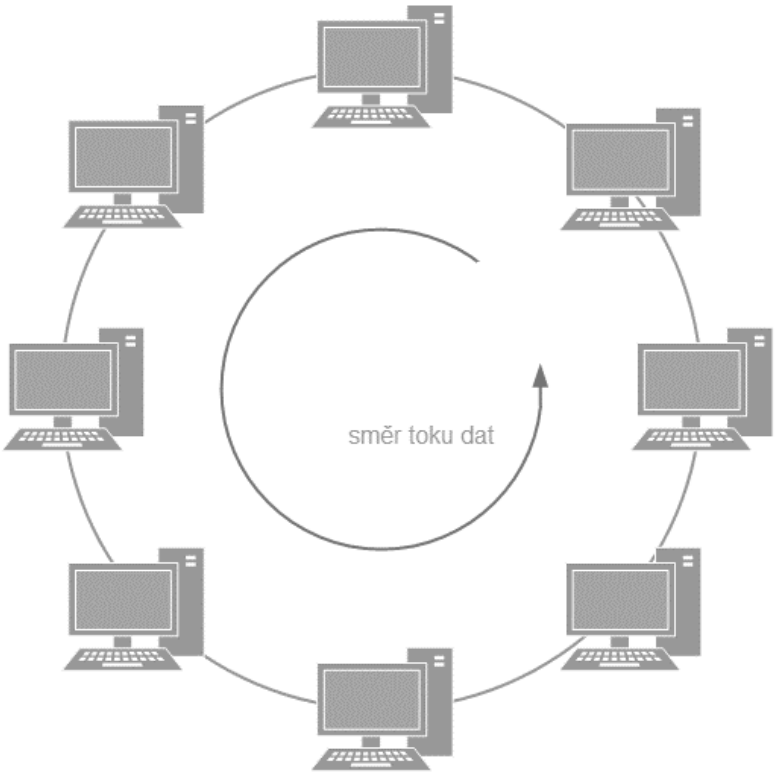


Obrázek 10 – Sběrnicová topologie

3.2.1.3 Kruhová topologie

Kruhová topologie (*Ring topology*) stejně jako sběrnicová, je topologií bez centrálního uzlu. Jednotlivé uzly (*stanice*) jsou propojeny pouze s předchozím a následujícím uzlem a tím vytváří kruh. Jako přenosové médium je zde využito opět koaxiálního kabelu, nebo optického kabelu. Data na této topologii jsou postupně předávána pouze jedním směrem od odesílatele

přes jednotlivé uzly až k příjemci, tudíž každý uzel slouží jako opakovač signálu. Největším záporem této topologie je případ, kdy dojde k výpadku jednoho uzlu, nebo přerušení přenosového média, a tím k výpadku celé sítě. [16, s. 38] [21, s. 133]



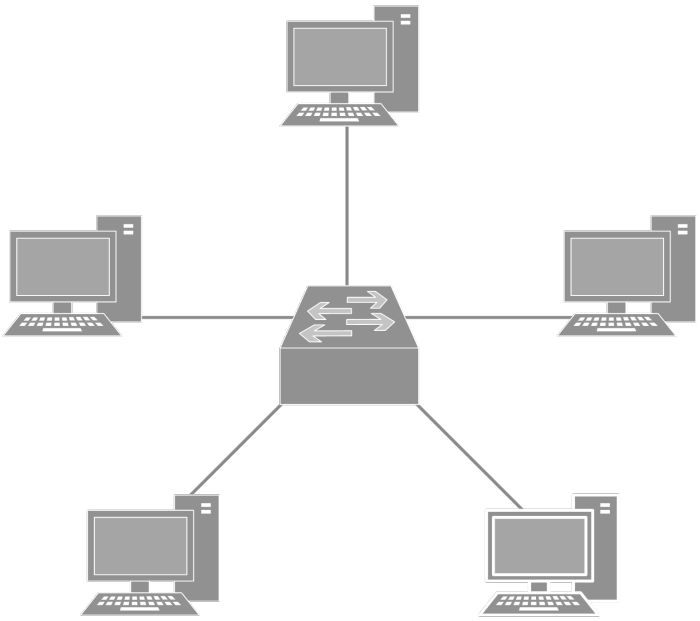
Obrázek 11 – Kruhová topologie

3.2.1.4 Topologie hvězdy

Topologie hvězdy (*Star topology*) je prvním případem topologie s centrálním aktivním či pasivním prvkem. Jednotlivé uzly (*stanice*) jsou propojeny pomocí přenosového média s centrálním prvkem. Pokud dojde k závadě na přenosovém médiu nebo na stanici, nemá to vliv na činnost sítě jako celku. Nefunkční je pouze daný uzel. Dojde-li však k závadě na centrálním prvku, potom dojde k výpadku celé sítě. V závislosti na použitém typu centrálního prvku se topologie hvězdy dělí na aktivní hvězdu nebo pasivní hvězdu. [21, s. 133]

Aktivní hvězda má ve svém středu SWITCH, pomocí kterého jsou data směrována k adresátovi. Data tedy neprochází celou sítí a jsou k dispozici pouze adresátovi. V pasivní hvězdě je centrálním prvkem HUB a data vyslaná do sítě jsou dostupná všem uzlům, ale rozumí jim jenom adresát. Pasivní hvězda je tedy jakousi degenerovanou sběrnicovou topologií, kdy přenosové médium ve sběrnicové topologii degenerovalo v jeden přípojný bod, kterým je ve hvězdě HUB. [16, s. 37]

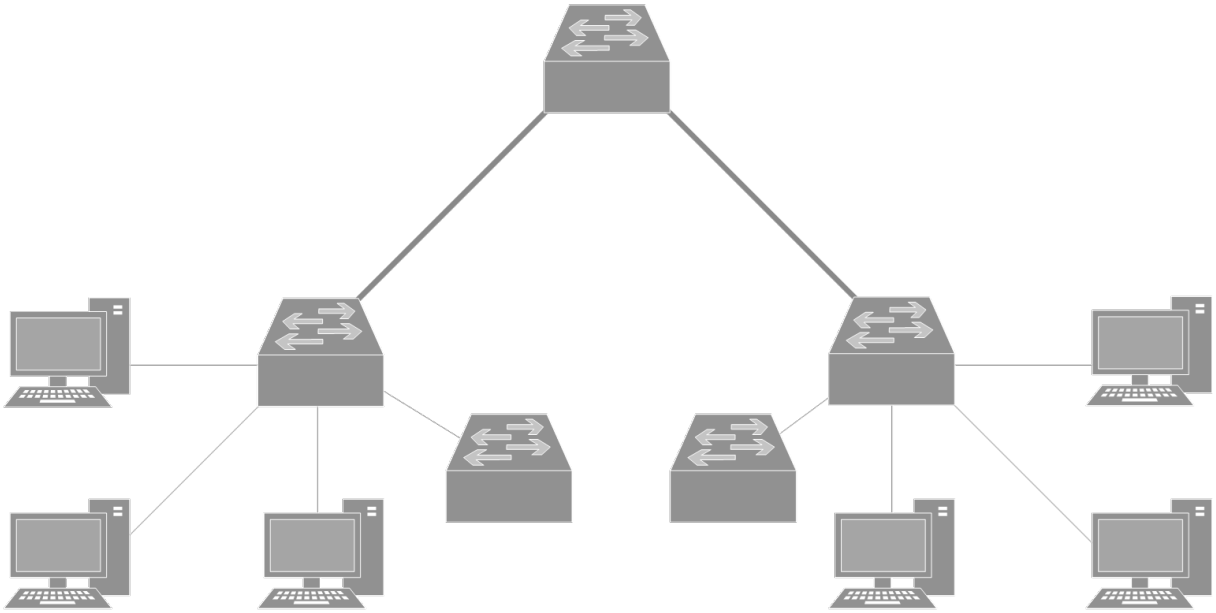
Nevýhoda této topologie je především ve velkém objemu spotřebované kabeláže a při selhání centrálního prvku výpadek celé sítě.



Obrázek 12 – Topologie hvězdy

3.2.1.5 Stromová topologie

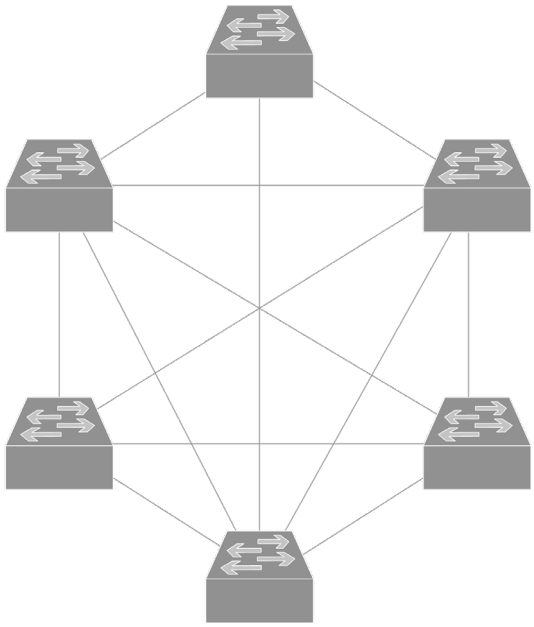
Stromová topologie (*Tree topology*) je vytvořena propojením více aktivních hvězd do jedné hierarchické struktury. Tato hierarchie je běžně využívána ve školách a větších firmách, kde jednotlivé hvězdy představují jednotlivá oddělení. Centrální prvky těchto jednotlivých oddělení jsou dále spojovány do hvězd až ke kořenu. [16, s. 38] [21, s. 133-134]



Obrázek 13 – Stromová topologie

3.2.1.6 Síť se smyčkami

Síť se smyčkami (*Mesh topology*) má dvě verze. První je plně propojená síť (*full mesh*), kdy každý uzel této topologie je propojen se všemi ostatními. V síti o „n“ uzlech se jedná o $\frac{n\times(n-1)}{2}$ spojů. Druhou verzí této topologie je částečně propojená síť (*partial mesh*). Zde jsou propojeny každý s každým jenom některé uzly, pro zbytek uzlů jsou některé spoje vynechány. Tato topologie se vyznačuje velkou spolehlivostí. To je dáno větším množstvím cest kudy mohou dva uzly mezi sebou komunikovat. [16, s. 38] [21, s. 134]



Obrázek 14 – Topologie částečný mesh

3.2.2 Logická topologie

U této topologie nezáleží na fyzickém rozmístění prvků, ale na způsobu přenosu dat a komunikaci mezi jednotlivými uzly (*stanicemi*) v síti. Nejvíce používanými logickými topologiemi jsou pro sdílené médium sběrnicová a kruhová topologie. Pro přímou komunikaci mezi dvěma uzly to je dvoubodové spojení neboli linka. [21, s. 134]

3.3 Rozdělení dle metody přístupu k médiu

V počítačových sítích se rozeznávají dva druhy metod v přístupu k médiu. První metodou je náhodný přístup (*stochastický*), jehož typickým představitelem je CSMA/CD (*Carrier – Sense Multiple Access with Collision Detection*). Druhou metodou je řízený přístup (*deterministický*) a představitelem je Token ring nebo Token bus. Podstatou těchto metod je v daném okamžiku zabezpečit vysílání pouze jedné stanice. V okamžiku, kdy vysílá více stanic

najednou dochází ke vzájemnému rušení, to má za následek nemožnost přenášet data v dané síti. [32, s. 26]

3.3.1 CSMA/CD

Tento typ přístupu je založen na rovnosti všech uzlů v síti. Neexistuje zde priorita pro vysílání. Uzly, které chtějí vysílat, naslouchají, zda na přenosovém médiu není provoz. Pokud provoz není, začnou vysílat, uspěje však pouze ten, který začal vysílat jako první. Díky zpoždění na médiu může nastat případ, kdy začne vysílat dva a více uzlů najednou, tím dojde ke kolizi. Uzel, který jako první zjistí tuto kolizi, vyšle speciální signál tzv. jam, kterým informuje ostatní stanice o zjištěné kolizi. Dojde k uvolnění přenosového média a uzly mohou začít opět vysílat. Uzly, které způsobily kolizi nezačínají vysílat okamžitě, ale odmlčí se na náhodně dlouhou dobu. S touto topologií pracuje především technologie ETHERNET. [16, s. 88] [21, s. 134] [32, s. 26]

3.3.2 Token ring

Principem této metody je předávání povolení k vysílání (*token*) a nutnost kruhové topologie. Uzly si toto povolení postupně předávají. Povolení k vysílání je časově omezené, pokud uzel nemá co vysílat, předává povolení dál. Vysílaná data si uzly postupně předávají mezi sebou do doby, než dorazí k adresátovi. Tuto topologii využívá především technologie TOKEN RING nebo FDDI (*Fiber Distributed Data Interface*). [21, s. 134-135] [32, s. 27]

3.3.3 Token bus

Princip této metody je obdobný jako u Token ring, jenom s tím rozdílem, že zde není podmínkou kruhová topologie. V síti, která používá tuto metodu, jsou stanicím přiděleny logické adresy, čímž dojde k vytvoření logického kruhu. Token si potom stanice postupně předávají dle posloupnosti této logické adresace. [32, s. 27]

3.4 Standardy sítí LAN

Z důvodu možnosti různého kombinování síťových prvků byly zavedeny standardy pro definování základních technických požadavků na realizaci sítí. Tyto standardy určuje organizace IEEE (*Institute of Electrical and Electronics Engineers*) a jednotlivé standardy jsou touto organizací označovány jako IEEE 802.XX. Kde číslo 802 značí rok (*1980*) a měsíc (*únor*) založení této organizace. Na pozicích XX se objevují číslice a písmena, označují jednotlivé

standardy sítí LAN. [16, s. 83] [32, s. 31] Tyto standardy jsou definovány dle následujících vlastností:

- přístupová metoda
- topologie
- charakteristika přenosového média
- rychlost přenosu dat

3.4.1 Ethernet (802.3X)

Ethernet navrhla v druhé polovině sedmdesátých let minulého století firma XEROX. V roce 1980 se XEROX spojil s firmami INTEL CORPORATION a DEC (*Digital Equipment Corporation*), z tohoto spojení vznikl Ethernet 1, který byl předán ke schválení IEEE jako standard. IEEE tuto verzi ethernetu vrátila k přepracování. Přepracováním vznikl Ethernet 2, označovaný také jako DIX Ethernet, a to podle počátečních písmen názvů společností, které ho vytvořili. I tuto přepracovanou verzi IEEE odmítla schválit, nicméně v roce 1983 použila Ethernet 2 jako základ pro svůj standard IEEE802.3.Ten se stal nejrozšířenějším standardem LAN sítí. Jelikož se obě verze, jak Ethernet 2 tak IEEE802.3, v dnešní době používají, je třeba mezi nimi důkladně rozlišovat. [16, s. 88] [32, s. 31] Následující popis se týká pouze standardu IEEE802.3.

Sítě typu Ethernet využívají jako metodu přístupu k přenosovému médiu CSMA/CD, a to především z důvodu použitého přenosového média a fyzické topologie. Pro stanice v síti Ethernet je charakteristická fyzická topologie sběrnice nebo hvězda. Jako přenosové médium pro první verze sloužil koaxiální kabel, v pozdějších (*novějších*) verzích tohoto standardu je použita jako přenosové médium kroucená dvoulinka (*angl. twisted pair*) a optické vlákno.

Značení jednotlivých verzí Ethernetu se lze rozdělit na tři části. První částí jsou číslice označující přenosovou rychlost standardu. Druhá část je vyjádřena slovem BASE nebo BROAD, která označuje pásmo, ve kterém standard pracuje. V případě BASE je to základní pásmo, respektive rozšířené pro BROAD. Třetí část informuje o přenosovém médiu (*F – optický kabel, T – kroucená dvoulinka, 2 (5) – maximální délka souvislého kabelu ve stovkách metrů*). [16, s. 92] [32, s. 32]

Standard 802.3 rozeznává následující 4 typy: Ethernet, Fast Ethernet, Gigabit Ethernet a 10GB Ethernet. [16, s. 92-103] [20, s. 183-185] [32, s. 32-35]

3.4.1.1 Ethernet (10BASE-X)

Jedná se o nejstarší verzi tohoto standardu, která existovala v následujících variantách:

- **10BASE-5 (802.3)** – jako přenosové médium byl použit „tlustý“ koaxiální kabel, který byl charakteristický svoji žlutou barvou. Maximální délka tohoto kabelu byla 500 metrů. Topologií byla sběrnice.
- **10BASE-2 (802.3a)** – sběrnicová topologie s přenosovým médiem „tenký“ koaxiální kabel, jehož maximální délka byla 185 m v jednom segmentu sítě. Délka celé sítě mohla být maximálně 910 m. Jeden segment sítě mohl obsahovat nanejvýš 30 uzlů a celá síť 1024 uzlů.
- **10BASE-T (802.3i)** – základem je nestíněná kroucená dvoulinka (*UTP – Unshielded Twisted Pair*), HUB nebo SWITCH a topologie hvězda. Maximální délka propojovacího kabelu mezi HUB a stanicí byla 100 m. Ve své době se jednalo o nejoblíbenější typ standardu IEEE 802.3.
- **10BASE-F (802.3j)** – přenosovým médiem bylo v této verzi optické vlákno. Tento typ měl tři specifikace:
  - **10BASE-FL (*fiber link*)** – specifikace určená především k propojování opakovačů, které mohli být maximálně čtyři v sérii.
  - **10BASE-FB (fiber backbone)** – specifikace určená pro páteřní spojení až 20 opakovačů.
  - **10BASE-FP (fiber passive)** – specifikace určená k připojení jednotlivých stanic.

3.4.1.2 Fast Ethernet (100BASE-X, IEEE 802.3u, y)

V roce 1993 byly vyvíjeny paralelně dva standardy pro zvýšení přenosové rychlosti v sítích LAN. Těmito standardy byly 100BASE-T a 100VG-AnyLAN. Pro svou jednoduchost a minimální odlišnost od již používaného standardu 10BASE-X byl zvolen jako vítězný standard 100BASE-T. [16, s. 94] Od standardu 10BASE-X se liší především nemožností použít jako přenosové médium koaxiální kabel a jako centrální prvek je výhradně použit switch. Tudíž fyzická topologie je pouze hvězda, a to přesněji hvězda aktivní. Tato verze standardu IEEE802.3 je realizována ve 4 verzích. [16, s. 95-96] [20, s. 184] [21, s. 169] [32, s. 32-33]

- **100BASE-T2** – jako přenosové médium slouží UTP kabel kategorie 3 a vyšší a využitými dvěma páry v UTP kabelu. Délka segmentu je maximálně 100 m.
- **100BASE-T4** – obdoba 100BASE-T2, pro přenos jsou využity 4 páry.

- **100BASE-TX** – přenosové médium je UTP kabel kategorie 5 s využitými dvěma páry v tomto kabelu. Je možné použít i kabel STP (*Shielded Twisted Pair*). Maximální délka segmentu je 100 m.
- **100BASE-FX** – přenosovým médiem jsou zde dvě optická vlákna, jedno pro vysílání a druhé pro příjem. Tato vlákna mohou být jednovidová (*SM – Single Mode*) nebo vícevidová (*MM – Multi Mode*). Délka segmentu se odvíjí od použitého typu vlákna.

3.4.1.3 Gigabit Ethernet (1000BASE-X, IEEE802.3z, ab)

Díky velké přenosové rychlosti v tomto standardu, je kladen velký důraz na kvalitu přenosového média. Verze IEEE802.3ab je definována pro metalické kabely a verze IEEE802.3z pro optické kabely. [16, s. 96-97] [20, s. 184] [21, s. 170] [32, s. 33-34]

- **1000BASE-T (IEEE802.3ab)** – tento typ standardu využívá jako přenosové médium kabel UTP kategorie 5 a 5e. Pro přenos jsou využity všechny 4 páry. Každý pár se využívá střídavě pro příjem a vysílání. Délka segmentu je maximálně 100 m.
- **1000BASE-TX (IEEE802.3ab)** – přenosové médium je kabel UTP kategorie 6, který využívá pro vysílání dva páry a zbylé dva pro příjem. Oproti 1000BASE-T je zapotřebí na vysílací i přijímací straně poloviční počet vysílačů, respektive přijímačů.
- **1000BASE-SX (IEEE802.3z)** – zdrojem světelného signálu je LED dioda (*Light Emitting Diode*) nebo laser. Přenosové médium je vícevidový optický kabel. Tento typ je využíván především pro kratší vzdálenosti přenosu.
- **1000BASE-LX (IEEE802.3z)** - jako zdroj světla je použit výhradně laser. Přenosové médium je jednovidový optický kabel. Pro přenos na vzdálenost do 5 km.

3.4.1.4 10GB Ethernet (IEEE802.3ae)

Zatím poslední a nejrychlejší verze Ethernetu, která je definována výhradně pro přenos po optických kabelech na velké vzdálenosti v řádu desítek kilometrů. Díky tomu je využitelná nejen v sítích LAN, ale také v sítích MAN a WAN. Tento standard nabízí sedm variant, které se od sebe liší použitým typem optického kabelu a typem sítě, pro kterou jsou určeny. Odlišnost značení těchto variant pro jednotlivé sítě je v použitém druhém písmenu za slovem BASE, kde

písmeno R označuje kódování 64 B/66 B pro sítě LAN a písmeno W znamená použití WIS (*WAN Interface Sublayer*). [16, s. 98-100] [20, s. 184-185] [32, s. 35]

- **10GBASE-SR** – standard určen pro sítě LAN, kde přenosovým médiem je MM optický kabel s přenosem do 300 m.
- **10GBASE-LR** – standard pro sítě LAN s optickým kabelem typu SM a přenosovou vzdáleností do 10 km.
- **10GBASE-ER** – standard pro sítě LAN s optickým kabelem typu SM a přenosovou vzdáleností do 40 km.
- **10GBASE-SW** – určeno pro sítě WAN, přenosové médium je MM optický kabel s přenosem do 300 m.
- **10GBASE-LW** – standard pro sítě typu WAN s MM optickým kabelem a přenosovou vzdáleností do 10 km.
- **10GBASE-EW** – standard pro sítě WAN s SM optickým kabelem a přenosovou vzdáleností do 40 km.
- **10GBASE-LX4** – standard pro oba typy sítí, který využívá tzv černé vlákno[7] (*dark fiber*), které může být jak MM, tak SM. Pro MM optický kabel je přenosová vzdálenost do 300 m a pro SM kabel je tato vzdálenost do 10 km.

3.4.2 Token Ring (802.5)

Síť typu Token Ring vyvinula v sedmdesátých letech minulého století firma IBM (*International Business Machines*), která později předala specifikace této sítě ke standardizaci společnosti IEEE. Na základě těchto specifikací vydala společnost IEEE standard 802.5. Na rozdíl od Ethernetu, tak verze této sítě od firmy IBM je totožná se standardem IEEE 802.5, tudíž jsou navzájem kompatibilní. Tento typ sítí je po Ethernetu druhým nejrozšířenějším typem lokálních sítí. [16, s. 106] [32, s. 35]

Sítě tohoto typu využívají jako přístupovou metodu k přenosovému médiu Token Ring, která spočívá v předávání tzv tokenu po logické topologii kruh. Vlastnictví tohoto tokenu opravňuje stanici k přístupu na přenosové médium a po určitý časový úsek vysílat. Pro dodržování předávání tokenu, zjišťování a opravu chybových stavů na přenosovém médiu plní jeden z uzlů, převážně první aktivní v kruhu, funkci aktivního monitoru. V případě poruchy

[7] Nevyužité optické vlákno, které vlastník pronajímá

nebo výpadku tohoto uzlu, automaticky přebírá funkci aktivního monitoru uzel jiný. [16, s. 106-107]

Fyzická topologie tohoto typu sítí je realizována v podobě hvězdy. Jako centrální prvek je zde jednotka zvaná MSAU (*Multi Station Attachment Unit*), což je obdoba HUB u sítí typu Ethernet. Tyto MSAU jednotky lze mezi sebou propojit, vždy ale do logického kruhu. Pro realizaci tohoto propojení jsou na těchto jednotkách speciálně vyhrazené porty, označené RI (*Ring In*) a RO (*Ring Out*). Ostatní porty slouží pro připojení jednotlivých stanic do již zmíněné hvězdy. Přenosovým médiem může být UTP, STP nebo optický MM, SM kabel. Délka UTP/STP kabelu pro připojení stanice k jednotce MSAU je maximálně 200 m, pro optický kabel je tato vzdálenost vyšší. Počet stanic v jednom segmentu sítě je stanoven normou na 255, u UTP kabelu dle použité kategorie 100-150 stanic. Přenosová rychlost byla původně 4 Mbit/s, později byla tato rychlost navýšena na 16 Mbit/s. U vysokorychlostního Token Ring se jedná o 100 Mbit/s. [16, s. 110-111] [32, s. 36]

4 Adresace v síti

Základní princip adresace spočívá v přidělení jedinečné adresy každému uzlu v síti, pomocí které je tento uzel jednoznačně identifikován. Tyto adresy jsou vyjádřeny v číselném tvaru, a to v desítkové, dvojkové nebo šestnáctkové číselné soustavě. Adresa v síti může označovat jeden nebo více uzlů. Pokud adresa označuje jeden uzel, jedná se o individuální adresu označovanou jako unicast. Jestliže adresa označuje více uzlů, potom jde o adresu skupinovou nebo všeobecnou. Pro skupinovou adresu se užívá označení multicast, v případě všeobecné to je broadcast. Adresování v sítích lze rozdělit do dvou základních skupin dle typu adresy, a to na adresování fyzické a logické. [16, s. 62] [20, s. 42]

4.1 Fyzické adresy

Pomocí fyzické adresy jsou jednotlivé uzly identifikovány pouze v místní síti. Tato adresa nijak nesouvisí s topologií dané sítě, v níž se uzel nachází, a to z důvodu toho, že fyzické adresování probíhá na linkové vrstvě RM ISO OSI, respektive vrstvě síťového rozhraní v TCP IP. Tento způsob adresace se nazýván jako plochá adresace. Fyzická adresa, označovaná také jako hardwarová nebo MAC, je přidělována kartám síťového rozhraní *(NIC – Network Interface Card*) během výrobního procesu (*BIA – Burned-In Address*) a je jedinečná na celém světe. Nachází se v paměti ROM (*Read Only Memory*) karet NIC a nelze ji měnit. Je tvořena 48 bity a reprezentována šesti dvojicemi hexadecimálních číslic, které jsou od sebe odděleny dvojtečkou nebo pomlčkou, popřípadě třemi čtyřčlennými skupinami hexadecimálních číslic oddělených od sebe tečkou. Struktura MAC adresy je rozdělena na dvě poloviny. Prvních 24 bitů, první tři dvojice čísel, se nazývá kód výrobce (OUI – Organizationally Unique Identifier) a je jednotlivým výrobcům přidělován centrálním správcem MAC adres, kterým je IEEE. Druhá polovina je přidělována výrobcem, který zaručuje jedinečnost této poloviny adresy. [16, s. 62-63, 79] [20, s. 42] [21, s. 157-158]

4.2 Logické adresy

Logická adresa neboli také IP adresa, slouží k jedinečné identifikaci uzlu v rámci celé sítě a k oddělování dané sítě od jiných sítí. Tato adresa na rozdíl od MAC adresy není pevná a je možné ji měnit. IP adresa je přidělována jednotlivým uzlům správcem dané sítě na základě topologie a použitého propojovacího zařízení (*switch, router*). Za logické adresování je odpovědný IP protokol, který plní dvě základní úlohy, kterými jsou adresování a fragmentace. Pro adresování je v dnešní době využíván protokol IP verze 4 (*IPv4*), který je však již nedostatečný a protokol IP verze 6 (*IPv6, IPng – Internet Protocol next generation*). [16, s. 63]

5 IPv4

Jedná se v pořadí o čtvrtou verzi ve vývoji protokolu IP a zároveň první verzi tohoto protokolu, která se široce rozšířila. Jako standard byla tato verze zavedena v roce 1981 a popsána v RFC 791, který nahrazuje původní RFC 760 z roku 1980. V roce 1993 došlo k úpravě tohoto standardu vydáním RFC 1517–1520. Tyto normy zavádějí do protokolu IPv4 nové mechanismy pro přidělování a práci s IP adresami. [23, s. 164,167]

Z důvodu jednoznačné identifikace jednotlivých uzlů a sítí tvůrce IP protokolu, sdružení IETF (*Internet Engineering Task Force*), rozhodl pro zavedení číselných adres. V protokolu IPv4 jsou adresy definovány jako 32bitové číslo. Toto číslo je rozděleno na čtyři 8bitová čísla, tzv. oktety, oddělena od sebe tečkou. První verze tohoto protokolu pracovala s tímto číslem v binární soustavě. Později bylo rozhodnuto o převodu z binární do desítkové soustavy, kde každý oktet může nabývat hodnoty od 0 do 255. Toto rozhodnutí bylo přijato pro usnadnění práce s těmito adresami pro běžné uživatele. Tento původní koncept protokolu umožňoval adresovat až 2^{32} (4 294 967 296) unikátních adres, což se z počátku považovalo za dostatečné a *nevyčerpatelné*. K zajištění toho, aby jedna IP adresa nebyla přidělena vícekrát, byl zaveden mechanismus, který toto zaručoval. Správcem tohoto mechanismu byla původně SRI NIC (*Stanford Research Institute – Network Information Center*), kterou později nahradila IANA (*Internet Assigned Numbers Authority*). Ta dále rozděluje IP adresy napříč celým světem regionálním organizacím, které tyto přidělené rozsahy dále rozdělují. Pro Evropu je touto organizací RIPE, APNIC pro Asii a Pacifik, ARIN pro oblast Severní Ameriky, LACNIC pro Střední a Jižní Ameriku a AFRINIC pro Afriku. V období devadesátých let minulého století, kdy došlo ke komercializaci internetu a zvýšila se poptávka po IP adresách, začalo být jasné, že tento počet adres nebude dostačující. Druhým důvodem velkého úbytku IP adres bylo v jejich způsobu přidělování. Společnost, která požádala o určitou množinu IP adres ji dostala bez kontroly, zda takový počet potřebuje či nikoli. Pro řešení těchto problémů byly zavedeny opatření, kterými jsou tvorba podsítí (*subnetting*), neveřejné adresování, CIDR (*Classless Inter Domain Routing*) a NAT (*Network Address Translation*). [21, s. 91] [33, s. 32-41, 109-112]

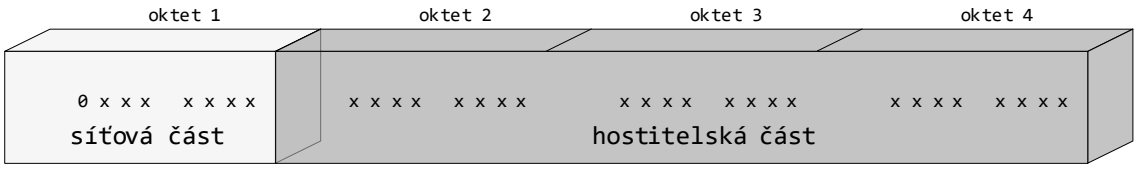
5.1 Rozdělení IP adres

Vnitřní struktura IP adresy je rozdělena na dvě části. První je část, která označuje adresu sítě. Tuto část přiděluje správce IP adres. Druhou část adresy přiděluje správce sítě a označuje jednotlivé uzly v dané síti. Toto rozdělení není fixní z jednoho prostého důvodu. Kdyby toto rozdělení bylo fixní například v poměru 50/50, tedy prvních 16bitů by určovalo síť a druhých

16bitů by určovalo jednotlivé uzly, potom by bylo možné v rámci protokolu IPv4 vytvořit pouze 2^{16}, tedy 65 536 jednotlivých sítí a v každé z nich pouze 2^{16} uzlů. Tímto rozdělením by vznikaly problémy pro velké sítě a docházelo by k plýtvání adresami v malých sítích. Z tohoto důvodu se autoři protokolu IP rozhodli vytvořit pět skupin IP adres, které se označují velkými písmeny A, B, C, D a E. V těchto třídách jsou jednotlivé oktety vyhrazeny pro síťovou a hostitelskou část v různých poměrech. Tím došlo k vyřešení problému velkých sítí, které čítají více jak 65 536 uzlů, tak k zamezení plýtvání adresami v malých sítích. [16, s. 250-252] [21, s. 86-89] [26, s. 127-133] [33, s. 36-40]

5.1.1 Adresy třídy A

Tato třída adres je využívána pro extrémně rozsáhlé sítě. Architektura této třídy adres spočívá ve využití pouze prvního oktetu pro část síťovou a zbylé tři pro část hostitelskou. První bit v první oktetu (*bajtu*) je v této třídě nastaven na hodnotu nula. Tímto je také zabezpečena jednoznačná identifikace této třídy adres v síti. V důsledku nastavení prvního bitu na hodnotu nula došlo k omezení možného počtu sítí. Pokud zbylé bity prvního oktetu jsou nastaveny na hodnotu jedna, výsledná adresa je 127.x.x.x, která je vyhrazena pro testování správné konfigurace protokolu IP jednotlivých uzlů, tzv *loop-back*. Další nepovolenou kombinací je nastavení zbylých bitů na hodnotu nula. Z tohoto omezení vychází číslo 126, které označuje možný počet sítí třídy A, rozsah adres je tedy v rozmezí od 1.0.0.0 do 126.0.0.0. Zbylé tři oktety (*24 bitů*) lze využít pro adresaci jednotlivých uzlů, z čehož vyplývá, že v každé síti třídy A je možné adresovat 2^{24} (16 777 216) jednotlivých uzlů. Od tohoto čísla je nutné odečíst adresy se samými nulami a jedničkami, které jsou vyhrazené. Tudíž skutečný využitelný počet uzlů pro každou síť třídy A je 16 777 214.

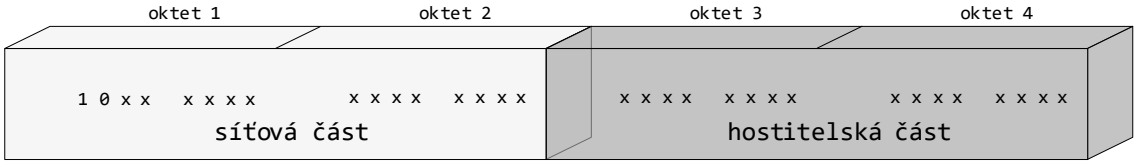


Obrázek 15 – Architektura IP adresy třídy A

5.1.2 Adresy třídy B

Tato třída adres je určena pro středně velké sítě. Pro síťovou část je v této třídě využito prvních dvou oktetů (*bajtů*) a zbylé dva oktety jsou určeny pro adresování jednotlivých uzlů v těchto sítích. Stejně jako u adres třídy A, tak i zde standard RFC požaduje povinné nastavení v prvním bajtu. Tentokrát se jedná o první dva bity, z nichž první bit je povinně nastaven na hodnotu 1 a druhý bit na hodnotu 0. Tímto omezením je počet možných sítí třídy B omezen na

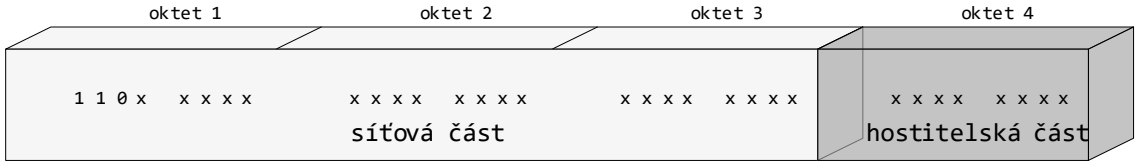
2^{14}, tedy na 16 384. Adresný prostor prvního oktetu je tímto omezen na hodnoty od 128.0.0.0 do 191.255.0.0. Pro adresování uzlů každé sítě třídy B je možno využít zbylých dvou bajtů, tedy 2^{16} uzlů. Po odečtení dvou adres se samými nulami a jedničkami je počet možných uzlů v každé síti třídy B 65 534.



Obrázek 16 – Architektura IP adresy třídy B

5.1.3 Adresy třídy C

U IP adres této třídy zabírá síťová část první tři oktety a zbylý čtvrtý oktet je určen pro adresování jednotlivých uzlů v těchto sítích. To dovoluje v každé síti této třídy adresovat 2^8 uzlů, po odečtení dvou zakázaných adres je tento počet 254. Z tohoto čísla vyplívá, že sítě této třídy jsou určené pro malé sítě. Standard RFC v této třídě požaduje nastavení prvních třech bitů v prvním oktetu na hodnoty první bit na hodnotu jedna, druhý bit na hodnotu jedna a třetí na hodnotu 0. Počet sítí třídy C je tedy roven číslu 2^{21}, tedy 2 091 152 možných sítí. Adresy této třídy v prvním bajtu mají hodnoty od 192.0.1.0 do 223.255.255.0.



Obrázek 17 – Architektura IP adresy třídy C

5.1.4 Adresy třídy D

Tato třída IP adres se od předešlých tříd odlišuje především svým účelem. Neslouží totiž k adresování sítí a uzlů, ale ke skupinové adresaci definovanou v RFC 1112. Z tohoto důvodu je i specifická architektura těchto IP adres, a to tak, že síťová část zde vůbec neexistuje. V prvním bajtu této třídy jsou povinně první tři bity nastaveny na hodnotu 1 a čtvrtý na hodnotu 0. Interval adres pro sítě této třídy je tedy v intervalu od 224.0.0.0 do 239.255.255.254.

Obrázek 18 – Architektura IP adresy třídy D

5.1.5 Adresy třídy E

Adresy této třídy jsou používány pouze pro výzkumné a experimentální účely organizací IETF. V prvním bajtu těchto IP adres jsou první čtyři bity nastaveny na hodnotu 1. Rozsah adres je v této třídě od 240.0.0.0 do 255.255.255.255.

5.2 Tvorba podsítí

Jeden z prvních mechanismů, který měl přispět ke zlepšení neefektivního přidělování IP adres. Dalším důvodem pro zavedení tohoto mechanismu bylo značné rozšíření počítačových sítí a fakt, že jednotlivé organizace začaly provozovat více sítí najednou. Organizace IETF proto hledala mechanismus, který by tuto situaci vyřešil. Bližší specifikace tohoto mechanismu lze najít v RFC 917. [33, s. 41-43]

5.2.1 Tvorba podsítí pomocí masky s pevnou délkou

Tvorba podsítí neboli subnetting spočívá ve zvětšení síťové části IP adresy na úkor hostitelské části IP adresy. Tento princip je popsán v RFC 950 a RFC 1812. Dle počtu požadovaných podsítí se z hostitelské části IP adresy v daném oktetu, dle třídy IP adresy, vezme potřebný počet bitů a těmito bity se prodlouží síťová část IP adresy. Tím se také sníží počet možných adresovatelných uzlů v dané podsíti. Pro tyto účely se využívá tzv. maska podsítě (*subnet mask*). Maska má stejný formát jako IP adresa, tedy 32bitové číslo rozdělené do čtyř oktetů. Pro každou třídu IP adres (A, B, C) je definována implicitní maska. V části masky, která odpovídá síťové část IP adresy jsou bity nastaveny na hodnotu 1 a pro část hostitelskou, jsou bity nastaveny na hodnotu 0. Adresa podsítě se vypočítá pomocí logického součinu bitů na stejných pozicích IP adresy a masky. Pro účely tvorby podsítí není však možné využívat libovolný počet bitů. Tento počet je omezen dle jednotlivých tříd IP adres. [16, s. 252-255] [21, s. 101-107] [33, s. 42-46]

- IP adresy třídy A mají implicitní masku v podobě 255.0.0.0 (binárně vyjádřeno: 1111 1111.0000 0000.0000 0000.0000 0000). Pro tvorbu podsítí lze použít bity 10-30, masky tudíž mohou být v rozsahu 255.192.0.0 – 255.255.255.252.
- Pro IP adresy je implicitní maska 255.255.0.0. Pro tvorbu podsítí, lze využít bity 18-30 a masky jsou v rozsahu 255.255.192.0 - 255.255.255.252.
- IP adresy třídy C mají implicitní masku 255.255.255.0. Pro tvorbu podsítí lze využít pouze bity 26-30. Masky jsou tudíž v rozsahu 255.255.255.192 – 255.255.255.252.

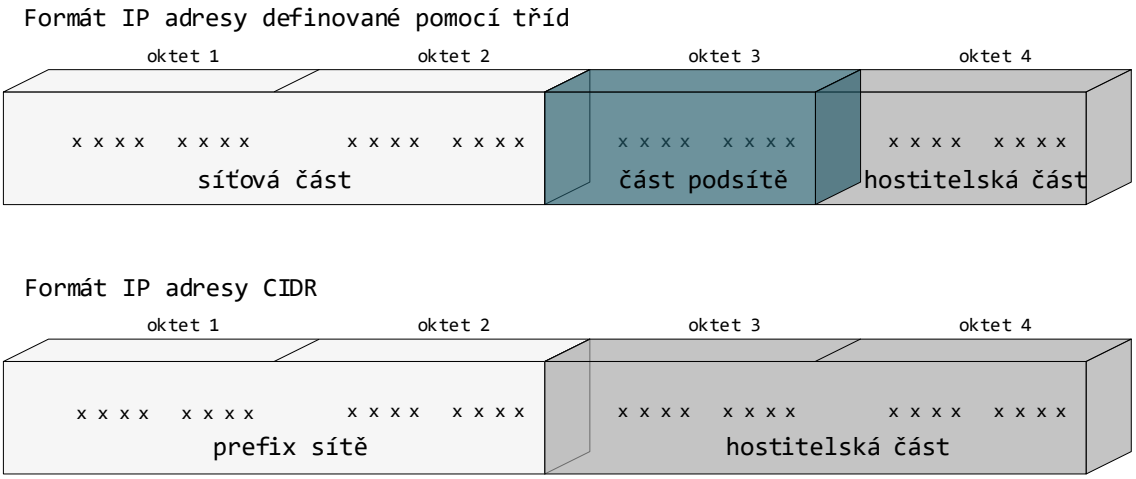
5.2.2 Tvorba podsítí pomocí masky s proměnnou délkou VLSM

Pro potřeby definování většího počtu podsítí s různým počtem adresovaných uzlů v podsíti byl v roce 1987 vydán dokument RFC 1009, kterým se umožňuje pro potřeby rozdělení podsítě využít vetší počet různých masek. Tento mechanismus byl nazván jako VLSM (*Variable Length Subnet Mask*). Princip spočívá v rozdělení IP adresy podsítě na další podsítě pomocí několika různých masek. Tímto způsobem lze z jedné podsítě vytvořit několik dalších podsítí, které mohou adresovat rozdílný počet uzlů, dle daných požadavků. Vytváření těchto podsítí se řídí postupem, pomocí kterého se vytvoří podsíť, která bude obsahovat nejvíce uzlů. Poté se vytvoří podsíť pro druhý největší počet uzlů. Tímto způsobem se pokračuje až k nejmenší potřebné podsíti. Nutno podotknout, že pro velikost podsítě se vždy hledá nejbližší číslo mocniny čísla dvě, které odpovídá počtu požadovaných IP adres uzlů v dané podsíti. Pro zjednodušení zápisu IP adresy sítě a její masky se využívá zápis IP adresy a prefixem. Prefix je lomítko s číslem za IP adresou. Toto číslo za lomítkem udává délku síťové části IP adresy (počet bitů) neboli počet jedniček v masce sítě z leva směrem doprava (př.: 192.168.12.192/26 – maska: 255.255.255.192). [16, s. 255-256] [33, s. 46-47]

5.3 CIDR

Na začátku devadesátých let minulého století došlo v rámci obrovského růstu internetu, a tudíž i poptávky po IP adresách ke krizi a vzrostly obavy, že IP adresy budou vyčerpány. Tento tzv. „*soudný den*“ měl nastav v březnu roku 1994. Tato obava a krize měly za následek poptávku po novém mechanismu přidělování IP adres, který by tento soudný den oddálil do doby zavedení nového protokolu IPng (*Internet Protocol Next Generation*). Tím se v roce 1993 stal mechanismus známý jako CIDR (*Classless Inter-Domain Routing*), neboli směrování na základě prefixu (*prefix routing*). Vlastní mechanismus je popsaný v RFC 4632, který nahrazuje původní RFC 1519, dále pak v RFC 1517, RFC 1518 a RFC 1520. Tento mechanismus přináší zásadní novinku, kterou je zrušení rozdělení IP adres do jednotlivých tříd. Místo rozdělení IP adres do jednotlivých tříd, které jasně definovalo dělící čáru mezi síťovou částí a hostitelskou částí IP adresy, umožňuje CIDR libovolnou polohu této dělící čáry v IP adrese. Poloha této

dělící čáry musí být vždy součástí IP adresy. Tohoto je dosaženo zápisem IP adresy s prefixem, který udává, kolik bitů z leva v IP adrese patří síťové části. [16, s. 256-257] [33, s. 48-50]



Obrázek 19 – Formát IP adres pomocí tříd a v rámci CIDR

5.4 Neveřejné adresy

Pro veřejné sítě platí, že každý uzel v této síti musí mít unikátní adresu pro jeho jednoznačnou identifikaci v této síti. Toto však neplatí pro sítě neveřejné neboli privátní, které nejsou k veřejným sítím připojeny nebo k těmto sítím přistupují přes určité zařízení, které tento přístup realizuje. Potom uzly v jedné privátní sítí mohou mít stejné IP adresy jako uzly v jiné privátní síti. Pro tyto potřeby byla definována skupina IP adres, která se v těchto privátních sítí využívá: [16, s. 252] [21, s. 89]

- ve třídě A byla vyhrazena 1 síť v rozsahu: 10.0.0.0 – 10.255.255.255
- ve třídě B bylo vyhrazeno 16 sítí v rozsahu: 172.16.0.0 – 172.31.255.255
- ve třídě C Bylo vyhrazeno 256 adres v rozsahu: 192.168.0.0 – 192.168.255.255

5.5 NAT

Překlad IP adres neboli NAT (*Network Address Translation*) definovaný v RFC 3022 je využit pro komunikaci uzlů z privátních sítí s uzly z veřejných sítí. V privátní síti musí existovat minimálně jedno zařízení (*router sloužící jako brána*), které má veřejnou IP adresu a přes které ostatní uzly privátní sítě komunikují s uzly ve veřejných sítích. Na tomto zařízení dochází k vlastnímu překladu IP adres. Princip spočívá v nahrazení privátní IP adresy v hlavičce odchozího paketu veřejnou IP adresou routeru (*brány*). Toto nahrazení zaznamená router do své tabulky překladu adres. V případě příchozího paketu vymění cílovou IP adresu, která je nastavena na veřejnou IP adresu daného routeru, za privátní IP adresu uzlu, kterému je paket určen, který mu je tento paket následně odeslán. Tuto privátní IP adresu zjistí z tabulky

překladu adres. Záznamy v této tabulce jsou vedeny pomocí přiřazení různého čísla portu ke každé dvojici privátní IP adresy odesílajícího uzlu a veřejné IP adresy routeru. [16, s. 257-258] [21, s. 90-91]

6 IPv6

Tato práce se protokolem IPv6 zabývá pouze okrajově, jelikož problematika tohoto protokolu je velice obsáhlá a vydala by na samostatnou práci. Zde bude představena pouze struktura IP adresy, ICMPv6 a DNS.

Jedná se o nástupce protokolu IP verze 4, jehož vznik se datuje na počátek devadesátých let minulého století. Potřeba nového protokolu byla hlavně z důvodu tenčícího se počtu volných IP adres protokolu IPv4. S ohledem na prognózy, které udávaly, že k vyčerpání IP adres protokolu IPv4 dojde nejdříve v roce 2005, se IETF rozhodla pro vytvoření protokolu, který přinese zásadní změny.

Požadavky na IPv6: [34, s. 23]

- Zvětšení prostoru adresace – vytvoření „nevyčerpatelného“ adresného prostoru
- Definování tří typů adres - individuální (unicast), skupinové (multicast) a výběrové (anycast)
- Jednotné adresy – pro veřejné a vnitřní sítě
- Směrování a adresace musí být hierarchické
- Bezpečnost - zahrnutí šifrování, autentizace a sledování cesty
- Vysoká kvalita podporovaných služeb
- Podpora vysokorychlostního směrování
- Plug and play konfigurace
- Mobilita
- Kompatibilita a nenáročný přechod z IPv4 na IPv6

Nový protokol dostal pracovní název IPng (*Internet Protocol next generation*), v roce 1995 byl vydán RFC 1883: *Internet Protocol Version 6 (IPv6) Specification*, který definuje základy IPv6. V následujících letech byly dále vydány RFC 2460, RFC 3775, RFC 8200 [34, s. 23-24]

6.1 Adresa IPv6

Podoba a struktura IP adresy protokolu IPv6 je definována v RFC 4291 (*IP Version 6 Addressing Architecture*). Oproti IP adrese protokolu IPv4, která je velká 32bitů, je IP adresa IPv6 definována jako 128bitové číslo. Z toho vyplývá, že v protokolu IPv6 je možné vytvořit 2^{128} ($3{,}4*10^{38}$) adres. Ta je rozdělena na dvě části, kde první část informuje o umístění

(*tzv. lokátor*). Tato část se využívá především pro směrování. Druhá část IP adresy slouží k identifikaci (*tzv. identifikátor*) zařízení nebo rozhraní. [16, s. 270] [33, s. 113]

Adresa se zapisuje pomocí osmi čtyřčíselných skupin v šestnáctkové soustavě, kde každá skupina reprezentuje 16bitů adresy. Jednotlivé skupiny jsou od sebe odděleny dvojtečkou. Z důvodu možné záměny některých písmen a číslic se jednotlivá písmena v IP adrese zapisují malými písmeny. Jelikož pro uživatele je tento zápis nepřehledný, očekává se ze strany uživatele výhradní používání služby DNS. Jediní, kteří by měli pracovat se zápisem IP adresy v šestnáctkové soustavě, budou správci sítí. Pro zápis samotné IP adresy existuje několik variant, a to především z důvodu existence velkého počtu nul v adrese. Tuto problematiku řeší RFC5952 (*A Recommendation for IPv6 Address Text Representation*) [16, s. 270-271] [34, s. 65-67]

- Plný zápis IP adresy: 2001:0000:0000:0db8:0000:0000:ac10:fe01
- Vynechání počátečních nul: 2001:0:0:0db8:0:0:ac10:fe01
- Zkrácený zápis: 2001::0db8:0:0:ac10:fe01, nebo 2001:0:0:0db8::ac10:fe01, nelze však 2001::0db8::ac10:fe01
- Speciální případ je adresa 0000:0000:0000:0000:0000:0000:0000:0000, kterou lze zkrátit pouze na: ::

Další možností zápisu IP adresy je pomocí prefixu, jehož způsob zápisu je převzat z CIDR IPv4. Tento způsob zápisu definuje příslušnost adresy do určité sítě nebo podsítě. Délka tohoto prefixu může být variabilní, a to z důvodu podrobnosti s jakou se na danou IP adresu nahlíží. Možnosti zápisu adresy s prefixem jsou následující: [34, s. 67-68]

- 2001:0000:0000:0db8:0000:0000:ac10:fe01/50
- 2001::0db8:0:0:ac10:fe01/50
- 2001:0:0:0db8::ac10:fe01/50

V protokol IPv6 jsou definovány tři skupiny IP adres, které se od sebe odlišují svým chováním. Jedná se o adresy jednosměrné (*unicast*), vícesměrné (*skupinové, multicast*), neadresné (*anycast*). [21, s. 95] [34, s. 65]

- Unicast adresa označuje konkrétní uzel v síti a data směrovaná na tuto adresu jsou doručena pouze tomuto uzlu
- Multicast adresa slouží pro adresování skupiny uzlů. Data odeslaná na tuto adresu jsou doručena všem uzlům ve skupině

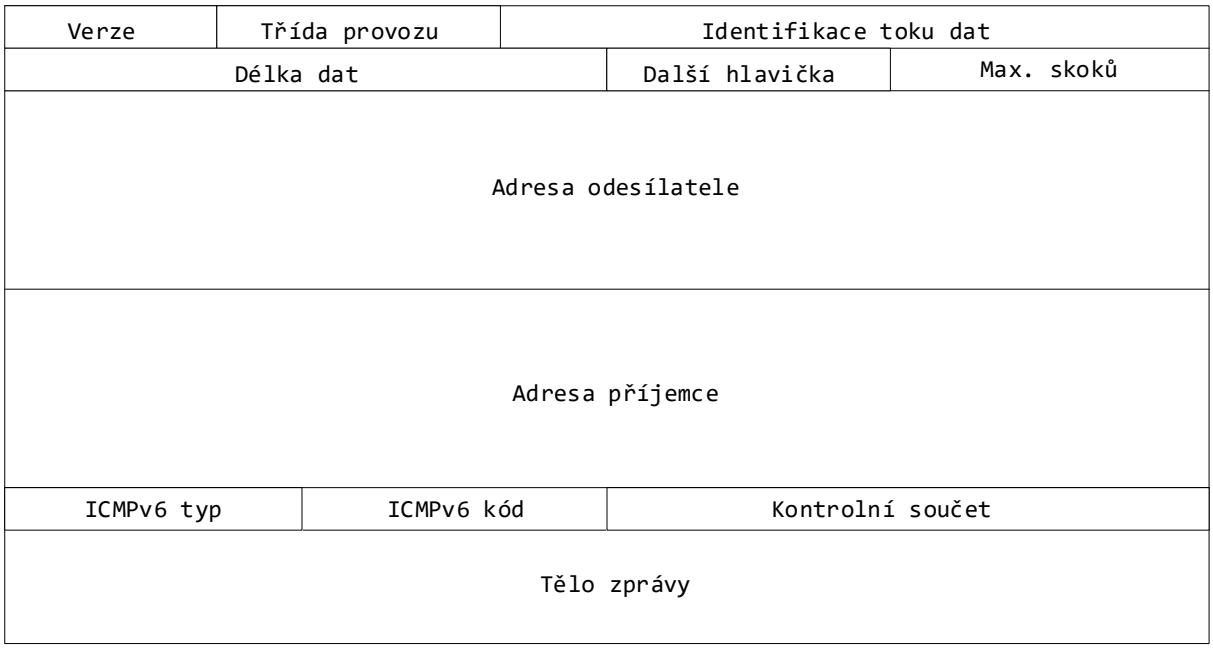
- Anycast adresa slouží podobně jako multicast adresa pro adresování skupiny uzlů s tím rozdílem, že data odeslaná na tuto adresu jsou doručena pouze jednomu uzlu, a to tomu nebližšímu

Obdobně jako u předchozí verze protokolu IP (IPv4), tak i v této verzi protokolu IP jsou předdefinovány určité skupiny IP adres. [16, s. 271] [34, s. 68-69]

- Nedefinovaná adresa ::/128
- Loopback ::1/128
- Unikátní individuální lokální adresy fc00::/7
- Individuální lokální linková adresy fe80::/10
- Skupinové (multicast) adresy ff00::/8
- Individuální globální adresy (RFC 2374) ostatní

6.2 ICMPv6

Jedná se o protokol sloužící k hlášení chyb a zjišťování dosažitelnosti rozhraní. Implementace tohoto protokolu je pro všechna zařízení používají IPv6 povinná. Základy ICMPv6 (*Internet Control Message Protocol version 6*) jsou definovány v RFC 4443: *Internet Control Message (ICMPv6) for Internet Protocol Version 6 (IPv6) Specification.* Zbylé komponenty tohoto protokolu jsou definovány v několika dalších RFC. Přítomnost zprávy ICMP v paketu je dána hodnotou 58 v položce *Další hlavička*. [16, s. 274] [34, s. 113]



Obrázek 20 – Datagram IPv6 s ICMPv6

Zprávy ICMPv6 se dělí do dvou tříd, a to na chybové a informační. Pro chybové zprávy je hodnota v poli ICMPv6 v rozmezí od 0 do 127 a pro informační zprávy je tato hodnota od 128 - 255.

6.2.1 Chybové zprávy

V současnosti ICMPv6 definuje pouze čtyři druhy chybových zpráv: [16, s. 274-275] [34, s. 115-117]

- Hodnota 1 – nedosažitelnost cíle. V příchozím datagramu na směrovač se vyskytuje IP adresa, na kterou tento paket nelze doručit.
- Hodnota 2 – příliš velký datagram. Velikost MTU (*Maximum Transmission Unit*) datagramu je větší než MTU linky, přes kterou má být odeslán.
- Hodnota 3 – vypršela doba platnosti datagramu. Počet skoků datagramu je roven nule, nebo příjemce neobdržel všechny fragmenty jednoho datagramu v daném časovém intervalu.
- Hodnota 4 – problém s parametry. Příjemce obdržel datagram, jehož parametrům nerozumí.

6.3 DNS

Účel DNS je převod IP adresy na název stránek nebo počítače a opačně. V případě protokolu IPv6 je DNS velice důležité především z důvodu dlouhého a obtížně zapamatovatelného zápisu IP adresy. Problematika DNS je řešena v RFC 3596: *DNS Extensions to Support IP Version 6*. [34, s. 215]

6.3.1 Dopředné dotazy

Dopředné dotazy slouží pro překlad názvu na IP adresu. V IPv4 pro tyto dotazy slouží záznamy typu *A,* a jelikož DNS pro IPv6 vychází z předešlé verze a IP adresa IPv6 je čtyřikrát delší, proto pro potřeby těchto dotazů jsou v IPv6 zavedeny záznamy typu *AAAA*. [34, s. 216]

6.3.2 Zpětné dotazy

Tento typ dotazu slouží k překladu IP adresy na název. Princip spočívá v plném zápisu IP adresy pozpátku a připojení domény *ipv6.arpa* na konec. Tímto způsobem se prefix dostane na konec a je možné realizovat distribuovanou správu reverzních domén. [34, s. 217-218]

7 Směrování

Pojmem směrování (*angl. routing*) se v oboru počítačových sítích označuje hledání nejefektivnější cesty pro doručení paketu adresátovi, který je v jiné síti, něž odesílatel. Pokud chce počítač komunikovat s jiným počítačem, který se ale nachází v jiné síti, komunikuje s ním přes zařízení nazývané směrovač neboli také výchozí brána (*angl. default gateway*). V takovéto komunikační cestě se může nacházet pouze jeden nebo více těchto směrovačů. Každý takovýto směrovač obsahuje tzv. směrovací tabulku (*angl. routing table*), podle níž rozhoduje kam jednotlivé pakety přesměrovat. Ve směrovací tabulce jsou zaznamenány jak cesty do sítí, které jsou přímo připojeny k jednotlivým rozhraním směrovače, tak i cesty do vzdálených sítí, kterých je možné dosáhnout pouze přes jiné směrovače. Cesty do těchto vzdálených sítí lze do routovací tabulky směrovače zapsat ručně, nebo se je směrovač může naučit skrze směrovací protokoly od ostatních směrovačů. Podle způsobu zapsání cesty do vzdálené sítě se rozlišuje statické nebo dynamické směrování. Společně s cestami je v routovací tabulce zaznamenávána i metrika těchto cest. Podle této metriky směrovač posuzuje, která z cest je pro daný paket výhodnější. Po přijetí paketu, směrovač z tohoto paketu odstraní hlavičku a porovná jeho cílovou adresu s adresami sítí ve své routovací tabulce. Pokud nalezne adresu sítě ve své routovací tabulce, přesměruje paket přímo na své rozhraní, ke kterému je daná síť připojena. Jestliže adresu sítě v tabulce nenalezne, přesměruje paket na takové své rozhraní, pro které má v routovací tabulce přednastavenu tzv. implicitní sít, která je pro tyto účely určena. Neexistuje-li v routovací tabulce cesta do implicitní sítě, je daný paket směrovačem zahozen. Další vlastnost paketu, kterou směrovač zkoumá, je jeho doba životnosti. Jedná se o číselnou hodnotu, která vyjadřuje počet směrovačů, přes které daný paket může projít. Každý směrovač, kterým daný paket projde tuto hodnotu sníží o jedničku. Pokud hodnota doby životnosti je větší jak jedna, paket je dále přesměrován. Rovná-li se však nule, je tento paket zahozen a odesílateli je odesláno chybové hlášení. [16, s. 315] [21, s. 69] [33, s. 27-29].

7.1 Statické směrování

Statické směrování je nejjednodušším typem směrování. Záznamy v routovací tabulce směrovače manuálně programuje administrátor sítě. Z toho plyne, že v případě statického směrování není možné dynamické vyhledávání alternativních cest v případě výpadku nebo poruchy sítě. Pro případy poruch sítě a rozložení zátěže, lze manuálně naprogramovat více statických cest současně. Tento druh směrování se využívá především v sítích s jednoduchou topologií, kde každá cesta vede většinou jenom do jednoho cíle. Statické směrování se dále využívá v případě, kdy chce síťový administrátor zajistit bezpečný přístup do nebo ze sítě. Dále

se toto směrování využívá pro nastavení cesty do implicitní sítě. Nastavení se provádí stejným způsobem jako nastavení jakékoli jiné cesty, jen s tím rozdílem, že adresa a maska sítě jsou nastaveny na hodnotu 0.0.0.0. Statické směrování lze kombinovat i s dynamickým směrováním jak v síti, tak i ve směrovači. V tomto případě má statické směrování přednost před dynamickým. Tato priorita lze změnit a využívá se jí především v okamžiku, kdy staticky definovaná cesta slouží jako záložní cesta pro případ selhání směrovacího protokolu. V důsledku chybějících jakýchkoli směrovacích protokolů je zatížení sítě tímto typem směrování nulové a zátěž samotného směrovače je minimální. [16, s. 317-318] [21, s. 69-71] [33, s. 145-148]

7.2 Dynamické směrování

V případě dynamického směrování, jsou záznamy v routovací tabulce zaznamenávány a aktualizovány pomocí směrovacích protokolů. Tyto protokoly se vždy snaží vybrat optimální cestu k dosažení cíle. Pro nalezení optimální cesty, každý protokol využívá jedno či více kritérií, dle kterých hodnotí všechny možné cesty k cíli. Tato kritéria se označují jako metrika. Mezi nejčastěji využívané metriky patří: [16, s. 319-320] [35, s. 492]

- Délka cesty (*angl. hop count*) – jedná se o počet směrovačů, který je mezi výchozím a cílovým uzlem. Nejlépe hodnocená cesta je ta s nejméně směrovači.
- Šířka pásma (*angl. bandwidth*) – udává největší možný objem dat, který je možné přes danou cestu poslat za určitý časový úsek. Optimální cesta je ta s největší minimální hodnotou šířky pásma. Udává se v kbit/s, Mbit/s.
- Zpoždění – Nejlépe ohodnocená cesta je ta s nejmenší hodnotou tohoto kritéria.
- Spolehlivost – toto kritérium udává pravděpodobnost doručení dat do cíle. Optimální cesta je ta, jejíž hodnota tohoto kritéria je největší.
- Zátěž – procentuální dynamické zatížení. Optimální cesta je ta, jejíž hodnota je nejnižší.
- MTU (*Maximum Transmission Unit*) – tato hodnota udává maximální velikost přenášené jednotky (paketu). Nejlépe ohodnocená cesta je ta s největší minimální MTU.
- Náklady – teoretické náklady související s danou cestou. Těmito náklady mohou být čas, obtížnost, riziko, nebo předešlé metriky. Tato hodnota je vyjádřena přirozeným číslem a nejlepší cesta je ta s nejmenší hodnotou tohoto čísla.

Samotné směrovací protokoly lze rozdělovat dle několika hledisek. Jedním z těchto hledisek je hledisko dle autonomního systému, dle kterého se směrovací protokoly dělí na vnitřní a vnější směrovací protokoly. Toto rozdělení lze jednoduše chápat tak, že vnitřní směrovací protokoly neboli také IGP (*Interior Gateway Protocols*), jsou využívány uvnitř autonomního systému. Naproti tomu vnější směrovací protokoly neboli EGP (*Exterior Gateway Protocols*), zajišťují směrování mezi jednotlivými autonomními systémy. [16, s. 320] [33, s. 144-145]

Dalším hlediskem pro rozdělení směrovacích protokolů je směrovací algoritmus. Dynamické směrování využívá dva základní směrovací algoritmy. Prvním je algoritmus vektorů vzdáleností (*angl. distance vector*), v němž si každý směrovač vypočítá vzdálenost ke každému cíli z informací (směrovacích tabulek), které obdržel pouze od svých sousedů. Druhým algoritmem je algoritmus stavu spojů (*angl. link state*). V tomto algoritmu si každý směrovač udržuje přehled o celé topologii sítě a veškeré informace o každém směrovači v této síti. Pro potřeby informovanosti si směrovače mezi sebou vyměňují oznámení o stavu linky (*LSA – Link State Advertisements*) [16, s. 320-324] [33, s. 148-151]

7.2.1 Směrovací protokol RIP

Protokol RIP (*Routing Information Protocol*) je nejstarší směrovací protokol postavený na algoritmech vektorů vzdáleností. Vyvinula ho v roce 1981 firma XEROX. Jedná se o protokol IGP, určený především pro malé a jednoduché sítě. Jeho první verze, tedy RIPv1, je popsána v RFC 1058 z června roku 1988. Vylepšená verze RIPv2, která nahradila RIPv1, je popsána v RFC 1723 z roku 1994. Nová verze protokolu přímo vychází z předchozí verze a přidává následující vylepšení: [16, s. 326-327] [33, s. 167-171, 201-207]

- Možnost VLSM
- Vysílání směrovacích informací na skupinovou adresu (224.0.0.9)
- Ověření pro směrovací tabulky

Metrika používaná tímto protokolem je délka cesty, tedy počet směrovačů na cestě. Nejvyšší hodnota je stanovena na hodnotu 15. Hodnota 16 již označuje neplatnou cestu. Metrika s nejnižšími hodnotami je určena pro sítě přímo připojené k jednotlivým rozhraním směrovače. Směrovací tabulka tohoto protokolu obsahuje síťovou adresu cíle, metriku, adresu směrovače (adresu rozhraní nejbližšího směrovače na cestě) a časovač (uplynulá doba od poslední aktualizace záznamu). Vysílací perioda směrovacích informací protokolu RIP je 30 s. Jestliže

informace nedorazí do 180 s, cesta je považována za neplatnou a daná cesta se v tabulce vymaže. [16, s. 326-327] [33, s. 176-184,202-206]

7.2.2 Směrovací protokol IGRP

Protokol IGRP (*Interior Gateway Routing Protocol*), stejně jako protokol RIP, vychází z algoritmů vektoru vzdáleností. Jedná se o směrovací protokol firmy CISCO a lze jej použít výhradně se směrovači této firmy. Protokol odstraňuje hlavní nedostatky protokolu RIP. Je určen pro IGP směrovače a umožňuje směrování čtyřmi různými cestami do jednoho cíle. Maximální délka cesty pro IGRP je 255 (počet směrovačů na cestě k cíli), implicitně je nastavena na hodnotu 100. Tento protokol dále využívá jiný typ metriky, označovaný jako kompozitní metrika. Nejvýhodnější cesta je určena na základě šířky pásma a zpoždění. Dále lze využít zátěž a spolehlivost, jako doplňující metriku. IGRP již není firmou CISCO podporován z důvodu nahrazení novějším protokolem EIGRP. [16, s. 328-329] [26, s. 401-402] [33, s. 218-221]

7.2.3 Směrovací protokol EIGRP

Obdobně jako protokol IGRP, tak i protokol EIGRP (*Enhanced Interior Gateway Routing Protocol*) je směrovací protokol firmy CISCO, který lze výhradně použít se směrovači této firmy. EIGRP vznikl jako rozšíření protokolu IGRP s podporou beztřídních adres. Dále tento protokol obsahuje nové technologie, kterými zefektivňuje svůj provoz a urychluje konvergenci sítě. Těmito technologiemi jsou: [16, s. 330] [33, s. 245-249]

- Obnova a rozpoznání sousedních směrovačů
- Nový přenosový protokol RTP
- Difuzní algoritmus DUAL
- Tři druhy tabulek – směrovací, topologie a sousední směrovače

Základem pro rozpoznávání a obnovování sousedních směrovačů je pravidelné rozesílání tzv. „hello“ paketu všem svým sousedům. Perioda rozesílání těchto hello paketů je 5 s. Těmito pakety směrovače zjišťují stav svých sousedů. [33, s. 249]

Protokol RTP (*Reliable Transport Protocol*) je transportní protokol vyvinutý firmou CISCO jako proprietární přenosový protokol jak pro spolehlivé, tak i nespolehlivé doručování zpráv protokolu EIGRP. [33, s. 250]

Nejdůležitější části EIGRP je difuzní algoritmus DUAL (*Diffusing Update Algorithm*). Jedná se o algoritmus, který se stará o všechny výpočty a porovnávání cest v protokolu EIGRP. Algoritmus vylučuje jakoukoli přítomnost smyček v cestách a pro směrovače, jichž se týká změna topologie sítě, provést aktualizaci cest v jednom okamžiku. Zbytek směrovačů v síti nic aktualizovat nemusí. [16, s. 330] [33, s. 250-251]

Pro svou potřebu EIGRP pracuje s větším počtem různých tabulek. V této práci jsou zmíněny pouze tři nejdůležitější. [33, s. 252-254]

- Tabulka sousedů – nejdůležitější tabulka. Protokol v této tabulce uchovává informace o přilehlých sousedních směrovačích a dále slouží jako podpora pro spolehlivé doručování paketů.
- Směrovací tabulka – pomocí DUAL jsou v této tabulce uloženy cesty ke všem známým cílům. Ke každému jednomu cíli je možné uložit až šest různých cest
- Tabulka síťové topologie – v této tabulce jsou uloženy informace potřebné pro výpočet vzdáleností do všech známých cílů.

7.2.4 Směrovací protokol OSPF

OSPF (*Open Shortest Path First*) je směrovací protokol postavený na algoritmu stavu spojů. Jeho poslední verze je popsána v RFC 2328. Základem tohoto protokolu je rozdělení sítě do oblastí (*angl. areas*). Toto rozdělení definuje tři druhy směrovačů v síti OSPF. Těmi jsou interní směrovače, hraniční směrovače oblastí a páteřní směrovače. S tímto rozdělením dále souvisí i dva typy směrování, kterými jsou směrování uvnitř oblasti a směrování mezi oblastmi. [16, s. 331] [33, s. 263-264]

Každý směrovač v síti OSPF si udržuje databázi stavů linek v síti. Počet databází směrovače je závislý na počtu oblastí, které daný směrovač propojuje. Aktualizace těchto databází je prováděna oznámením o stavu linky LSA (*Link State Advertisements*). Tyto LSA rozesílají směrovače všem svým sousedním směrovačům v dané oblasti. Z těchto informací si směrovač skládá aktuální podobu sítě oblasti, ve které je umístěn. Tato podoba sítě je ve formě stromu nejkratších cest, kde daný směrovač je kořenem tohoto stromu. Cesty do jiných sítí jsou v tomto stromu listy. Tyto optimální cesty jsou vypočteny pomocí Dijkstrova algoritmu, který zároveň odstraňuje smyčky v topologii. [16, s. 331-334] [33, s. 265-268]

Metrika v tomto protokolu je označována jako cena a je reprezentována číslem od 1 do 65535. Cena každé linky se vypočítá jako podíl 10^8 a šířky pásma dané linky. Čím je číslo menší tím je linka kvalitnější, a tudíž i preferovanější. [16, s. 335] [26, s. 451]

8 Přenosová média

Přenosová média slouží k přenosu, přesněji řečeno k šíření signálu. Jsou to prvky sítě, které se svojí činností aktivně nepodílejí na přenosu dat v síti. Z tohoto důvodu jsou označována jako pasivní prvky sítě. Existují dva základní typy přenosových medií, drátové a bezdrátové. Mezi drátová přenosová média se řadí koaxiální kabely, symetrické kabely a optické kabely. U bezdrátových se jedná především o šíření elektromagnetických vln prostorem kolem nás.

8.1 Koaxiální kabel

Jedná se o nesymetrický kabel, což znamená, že kabel má jeden vnitřní vodič a jeden vnější (stínění). Tyto dva vodiče jsou od sebe odděleny nevodivou vrstvou a celý kabel je chráněn plastovým pláštěm. Pro připojení k tomuto médiu se využíval BNC konektor. Tento druh přenosového média byl v sítích využívám především v dřívějších dobách. V dnešní době se toto médium prakticky nevyužívá. V počítačových sítích rozeznáváme tenký a tlustý koaxiální kabel. [16, s. 30-31] [21, s. 20-21]

8.1.1 Tenký koaxiální kabel

Nahradil dříve používaný tlustý koaxiální kabel. Tenký koaxiální kabel je tvořen vnitřním vodičem, izolací a jednou vrstvou stínění. Oproti tlustému koaxiálnímu kabelu je jeho průměr poloviční, cca 5mm, a tudíž je i mnohem flexibilnější a levnější. Využívá se pro kratší vzdálenosti, cca 185 metrů, s přenosovou rychlostí 10Mbps. [16, s. 25] [21, s. 21]

8.1.2 Tlustý koaxiální kabel

Tlustý neboli také žlutý koaxiální kabel je tvořen vnitřním vodičem, izolací a čtyřmi vrstvami stínění. Žlutý se mu říkalo z toho důvodu, že jeho vnější plastový obal byl vyráběn výhradně ve žluté barvě. Z důvodu vnitřní konstrukce byl tento kabel málo ohebný a obtížný na instalaci. Přenosová rychlost je 10Mbps na vzdálenost 500 metrů, poté musí být použit opakovač signálu. [16, s. 25] [21, s. 21]

8.2 Symetrický kabel (kroucená dvojlinka)

Tento kabel nahradil koaxiální z důvodu rychlosti a spolehlivosti. Je tvořen čtyřmi různobarevnými páry vodičů, které jsou po celé svojí délce pravidelně zkrouceny. Každý pár je zkroucen jiným způsobem. Výsledné zkroucené páry jsou společně znovu zkrouceny. Kroucení se provádí z důvodu eliminace elektrických přeslechů. Pro tento vodič se používá koncovka RJ-45. Při osazování kabelu touto koncovkou je možné zvolit ze dvou typů instalace. Tyto dva

typy osazení vycházejí z norem TIA/EIA 568-A a TIA/EIA 568-B. Dle použité normy na každém konci kabelu je rozlišován kabel přímý a kabel křížený. V případě rovného kabelu je na obou koncích použita stejná norma. Pokud se jedná o křížený kabel, tak na každém konci je použita odlišná norma. Symetrický kabel rozdělujeme do dvou základních skupin, a to stíněné a nestíněné. [21, s. 14,19] [32, s. 13,16-17]

8.2.1 Symetrický kabel nestíněný

Symetrický kabel, nemá stíněné kroucené páry – UTP *(Unshielded Twisted Pair*). Vhodný pro použití v domácnostech a v kancelářích, kde se vyžadují nízké náklady.

8.2.2 Symetrický kabel stíněný

Prvním typem je symetrický kabel, který má stíněné jednotlivé páry a tyto páry jsou opleteny dalším stíněním – STP (*Shielded Twisted Pair*). Druhým typem je kabel, který nemá stíněny jednotlivé páry, ale pouze stínění všech párů – ScTP (*Screened Twisted Pair*). Používá se pro vysoké přenosové výkony a na místech, kde se může vyskytovat elektromagnetické rušení. [21, s. 14-15] [32, s. 14,16]

8.2.3 Kategorie symetrického kabelu

V současné době je známo celkem devět následujících kategorií symetrického kabelu: [21, s. 16-17] [32, s. 14] [36]

- Cat.1 – nevyužívá se k datovým přenosům, ale hlavně pro telefonní rozvody. Rychlost přenosu do 1Mbit/s.
- Cat.2 – určena pro přenos dat, hlavně zvuku, s šířkou přenosového pásma do 1,5Mhz. Přenosová rychlost do 4 Mbit/s.
- Cat.3 – používaný pro telefonní rozvody. Přenosová rychlost do 16Mbit/s. Označován jako 10BASE – T a 100BASE – T4.
- Cat.4 – obdobný kategorii cat.3, byl však velmi brzo nahrazen cat.5.
- Cat.5 – kategorie je označována jako 100BASE – TX 1000BASE – T. Šířka přenosového pásma je u této kategorie 100MHz, maximální délka vedení je 100 m a maximální přenosová rychlost je 1Gbit/s. V dnešní době nahrazen cat.5E.
- Cat.5e – rozšířená verze cat5, která pro přenos používá všechny čtyři páry. Dnes nejvíce rozšířená. Označení 100BASE – TX 1000BASE – T.

- Cat.6 – kabeláž pro nově budované rozvody. Rychlost přenosu je 1 Gbit/s a šířka přenosového pásma je 250MHz. Využívá se hlavně pro ultrarychlé páteřní sítě. Označení 1000BASE-T, 1000BASE-TX.
- Cat.6e – kategorie bez omezení délky kabelu. Šířka přenosového pásma je 500MHz a přenosová rychlost je 10Gbit/s. Označení 10GBASE-T, 1000BASE-T, 1000BASE-TX.
- Cat.7 vyžadována kabeláž typu F a konektor GG45, TERA. Šířka pásma je 600MHz, přenosová rychlost 10 Gbit/s a délka kabelu není omezena. Označení 10GBASE-T, 1000BASE-T, 1000BASE-TX.

8.3 Optický kabel

Jako přenosové médium je zde využito skleněné nebo plastové vlákno, které za pomoci šíření světla v něm, přenáší signál. Jako zdroj je zde využita laserová dioda, nebo LED (*Light Emitting Diode*) dioda. Tento typ kabeláže je naprosto odolný vůči elektromagnetickému rušení. Pro počítačové sítě se používají dva základní typy optických vláken, a to jednovidová (*single mode*) a mnohavidová (*multimode*). [20, s. 31] [32, s. 18-19]

8.3.1 Single mode optické vlákno

V tomto typu vlákna se může šířit jenom jeden paprsek světla, a to díky malému průměru jádra, který činí 9 µm. Jako zdroj světla se zde používá laserová dioda. Pro tyto kabely je typická žlutá barva. [20, s. 32] [21, s. 23]

8.3.2 Multimode optické vlákno

V tomto typu vlákna se šíří více paprsků světla, které se odrážejí každý pod jiným úhlem odrazu. Průměr jádra je zde 50 µm nebo 62,5 µm a jako zdroj světla je zde použita LED dioda. Označení je buď oranžovou barvou, nebo modro-zelenou barvou. [20, s. 32] [21, s. 23]

8.4 Bezdrátové připojení

Typ propojení mezi jednotlivými uzly v síti, za pomoci bezdrátové technologie. Nejčastěji za pomoci šíření elektromagnetických vln v prostoru kolem nás. Tato připojení se označuje jako Wi-Fi (Wireless Fidelity) a jsou definována pomocí standardu IEEE 802.11. Následují příklady vybraných typů standardu. [16, s. 117-119] [32, s. 52-53]

- IEEE 802.11a – maximální přenosová rychlost 54 Mbit/s v pásmu 5GHz.
- IEEE 802.11b – maximální přenosová rychlost 11 Mbit/s v pásmu 2,4 GHz.

- IEEE 802.11g – maximální přenosová rychlost 54 Mbit/s v pásmu 2,4 GHz.
- IEEE 802.11n – maximální přenosová rychlost 600 Mbit/s v pásmu 2,4 a 5 GHz.
- IEEE 802.11ac – maximální přenosová rychlost 1800 Mbit/s v pásmu 5GHz.

9 Síťová zařízení

Síťová zařízení neboli také aktivní prvky sítě jsou takové prvky, které se svojí činností přímo podílejí na přenosu dat v síti nebo určitým způsobem ovlivňují dění v síti.

9.1 Repeater

Tato zařízení pracují na nejnižší vrstvě síťového modelu (fyzické) a jejich hlavním úkolem je zesílení signálu, který tímto zařízením prochází. Repeater se používá tam, kde délka vedení je už tak velká, že na konci tohoto vedení by byl signál velmi slabý. Zpravidla obsahuje dva porty. Jedním portem přijímá signál, který má zesílit a druhým portem tento zesílený signál vysílá. Najdeme ho především v sítích, kde se jako přenosové médium využívá koaxiální kabel. Celkový počet těchto zařízení v síti je omezen na 4. [16, s. 297-299] [21, s. 26] [32, s. 28]

9.2 Media konvertor

Toto zařízení slouží v síti k tomu, aby převedlo určitý typ přenosového média na jiný (optický kabel na symetrický kabel), další funkcí je zesílení signálu. [32, s. 28]

9.3 Switch

Zařízení, které obsahuje více síťových portů, do kterých se připojují síťová zařízení nebo jiné části počítačových sítí. Switch se sám učí MAC adresy zařízení připojených k jednotlivým portům. Tyto záznamy, tedy MAC adresu a příslušný port, ukládá do tabulky, kterou dynamicky aktualizuje. Při komunikaci mezi jednotlivými zařízeními switch přepíná komunikaci jenom požadovaným směrem a nezahlcuje touto komunikací zbytek sítě. To znamená, že je vytvořeno spojení jenom mezi těmi zařízeními, které spolu chtějí komunikovat. Switch může pracovat v několika režimech, ve kterých zpracovává přijatá data. Těmito režimy jsou ulož a pošli (*angl. store and forward*), průběžné zpracování (*angl. cut through*) a s omezením malých rámců (*angl. fragment free*): [16, s. 307-308] [21, s. 28-29] [32, s. 28-29]

- Metoda ulož a pošli – načte a uloží celý datový rámec, zkontroluje výchozí a cílovou MAC adresu a neporušenost dat, která je dána kontrolním součtem daného rámce. Pokud je vše v pořádku pošle rámec dál. Tímto zabraňuje šíření chybných rámců v síti. Jedná se o nejpomalejší metodu.
- Metoda průběžného zpracování – příchozí rámec je odeslán ihned poté, co switch obdržel dostatečnou část rámce, ze které je schopen zjistit cílovou MAC adresu. Tato metoda žádným způsobem nekontroluje neporušenost rámců. Jedná se o nejrychlejší metodu.

- Metoda s omezením malých rámců – jedná se o kompromis mezi oběma předchozími metodami. Příchozí rámec se začíná zpracovávat až ve chvíli, kdy switch obdrží prvních 64 bytů. Tímto způsobem je zajištěno, že se nejedná o poškozený rámec.

9.4 Router

Jedno z nejinteligentnějších zařízení v síti. Na rozdíl od switche, který umí propojit zařízení jenom ve stejné síti, router propojuje zařízení z různých sítí. Nejběžnější použití je v sítích WAN a v lokálních sítích (pomocí routeru se lokální sítě připojují k internetu). S tímto aktivním prvkem také souvisí pojem směrování (routování). Směrování má za úkol volbu co nejefektivnější cesty dat v sítí. [21, s. 30] [32, s. 29] Podrobnější činnost směrovače a způsoby směrování jsou rozebírány v kapitole 7 této práce.

9.5 Gateway

Tento aktivní prvek stojí na vrcholu v počítačových sítích, jelikož pracuje na úrovni aplikační vrstvy. Obsahuje tedy všechny vrstvy síťového protokolu. Gateway propojuje sítě, které pracují s navzájem odlišnými komunikačními protokoly. [16, s. 343]

10 Závěr

Cílem této práce bylo popsání vybraných základních principů počítačových sítí a vytvoření podpory pro orientaci nových pracovníků na pracovišti CIS u VÚ7214 v oblasti počítačových sítí pro možnost jejich dalšího vzdělávání v tomto oboru.

Jednotlivé části a kapitoly jsou koncipovány tak aby na sebe postupně navazovaly. V první části byla shrnuta historie a vývoj počítačových sítí. Byl vysvětlen rozdíl mezi síťovým modelem RM ISO OSI a architekturou TCP a popsány funkce jejich jednotlivých vrstev. V dalších kapitolách byly rozebírány topologie sítí, standardy v sítích LAN a způsob adresace v těchto sítích.

Druhá část se zabývala síťovým protokolem IPv4 a jeho nástupcem IPv6. V části týkající se IPv4 byla popisována IP adresa používaná v tomto protokolu. Dále pak třídy této IP adresy a způsob tvorby podsítí. Část zabývající se IPv6 byla oproti části IPv4 popsána stručněji, a to z důvodu složitosti celé problematiky kolem tohoto protokolu. Poslední kapitolou v prostřední části této práce byla kapitola zabývající se směrováním. Bylo zde vysvětleno statické, dynamické směrování a základní principy vybraných směrovacích protokolů.

Ve třetí části byly stručně představeny aktivní a pasivní prvky, které se využívají v počítačových sítích. V části pasivních prvků byly popisovány základní charakteristiky přenosových médií, jakými jsou koaxiální kabel, kroucená dvoulinky, optický kabel a Wi-Fi. V poslední kapitole této práce byly popisovány funkce jednotlivých aktivních prvků, které se mohou nacházet v počítačové síti.

Dle mého názoru a výše uvedeného popisu práce splnila stanovené cíle. Byl vytvořen pokladový studijní materiál, který pomůže novým pracovníkům při jejich dalším vzdělávání v oboru počítačových sítí.

11 Bibliografie

[1] SAGE: SEMI-AUTOMATIC GROUND ENVIRONMENT AIR DEFENSE SYSTEM. *MIT Lincoln Laboratory* [online]. LINCOLN LABORATORY, MASSACHUSETTS INSTITUTE OF TECHNOLOGY: LINCOLN LABORATORY, 2020 [cit. 2020-03-11]. Dostupné z: https://www.ll.mit.edu/about/history/sage-semi-automatic-ground-environment-air-defense-system

[2] 7.3 SAGE (Semi-Automatic Ground-Environment Computers) | Bit by Bit. *Bit by Bit* [online]. [cit. 2020-03-11]. Dostupné z: http://ds-wordpress.haverford.edu/bitbybit/bit-by-bit-contents/chapter-seven/7-3-sage-semi-automatic-ground-environment-computers/

[3] Sage: The First National Air Defense Network. *SAGE: The First National Air Defense Network* [online]. IBM [cit. 2020-03-11]. Dostupné z: https://www.ibm.com/ibm/history/ibm100/us/en/icons/sage/

[4] MUSIL, Marek. Vývoj Internetu - Nultá fáze. *Vývoj Internetu* [online]. Plzeň, b.r. [cit. 2020-03-19]. Dostupné z: http://ihistory.webzdarma.cz/chap/0faze.php

[5] MUSIL, Marek. Historie sítě Internet. *Vyvoj site Internet* [online]. Plzeň, b.r. [cit. 2020-03-11]. Dostupné z: http://ihistory.webzdarma.cz/chap/vyvoj.php

[6] SMYSITELOVÁ, Lucie. Historie rozlehlých počítačových sítí. *Historie rozlehlých počítačových sítí* [online]. 1999 [cit. 2020-03-11]. Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/xsmysit.html

[7] PETERKA, Jiří. Na počátku byl ARPANET .... *EArchiv: Archiv článků a přednášek Jiřího Peterky* [online]. 1995 [cit. 2020-03-11]. Dostupné z: https://www.earchiv.cz/a95/a504c502.php3

[8] MUSIL, Marek. 1. fáze INTERNETU. *Historie sítě Internet* [online]. Plzeň, b.r. [cit. 2020-03-19]. Dostupné z: http://ihistory.webzdarma.cz/chap/1faze.php

[9] Cybertelecom :: Internet History 80s. *Cybertelecom :: Federal Internet Law and Policy* [online]. Cybertelecom, 2019 [cit. 2020-03-11]. Dostupné z: http://www.cybertelecom.org/notes/internet_history80s.htm#csnet

[10] CSNET, Computer Science Network. *Internet history, design, advanced use, help, security, important features...* [online]. b.r. [cit. 2020-03-11]. Dostupné z: https://www.livinginternet.com/i/ii_csnet.htm

[11] CSNET - The History of Domain Names. *Home - The History of Domain Names* [online]. Bellevue: The History of Domain Names, b.r. [cit. 2020-03-11]. Dostupné z: http://www.historyofdomainnames.com/csnet/

[12] Cybertelecom :: NSFNET. *Cybertelecom :: Federal Internet Law and Policy* [online]. Cybertelecom, 2019 [cit. 2020-03-11]. Dostupné z: http://www.cybertelecom.org/notes/nsfnet.htm

[13] NSFNET - The History of Domain Names. *Home - The History of Domain Names* [online]. Bellevue: The History of Domain Names, b.r. [cit. 2020-03-11]. Dostupné z: http://www.historyofdomainnames.com/nsfnet/

[14] A Brief History of NSF and the Internet. *NSF - National Science Foundation* [online]. Virginia, 2003 [cit. 2020-03-11]. Dostupné z: https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050

[15] US NSF - NSF and the Birth of the Internet. *NSF - National Science Foundation* [online]. Virginia, b.r. [cit. 2020-03-11]. Dostupné z: https://nsf.gov/news/special_reports/nsf-net/1980.jsp

[16] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z: [technologie pro datovou, hlasovou i multimediální komunikaci]*. 2., aktualiz. vyd. Brno: Computer Press, 2006. ISBN 80-251-1278-0.

[17] PETERKA, Jiří. Jiří Peterka: Báječný svět počítačových sítí, část III. - Síťové architektury. *EArchiv: Archiv článků a přednášek Jiřího Peterky* [online]. 2005 [cit. 2020-03-11]. Dostupné z: https://www.earchiv.cz/b05/b0500001.php3

[18] Protokolová datová jednotka. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2020-03-20]. Dostupné z: https://cs.wikipedia.org/wiki/Protokolov%C3%A1_datov%C3%A1_jednotka

[19] BOUCHALA, Petr. Počítačové sítě. In: *PB pro SŠ* [online]. Havířov: Petr Bouchala, b.r. [cit. 2020-03-22]. Dostupné z: http://boucpe.wz.cz/et3/psi2.pdf

[20] PUŽMANOVÁ, Rita. *Širokopásmový Internet: přístupové a domácí sítě*. Vydání první. Brno: Computer Press, 2004. ISBN 80-251-0139-8.

[21] SPURNÁ, Ivona. *Počítačové sítě: praktická příručka správce sítě*. Vydání první. Kralice na Hané: Computer Media, 2010. ISBN 978-80-7402-036-0.

[22] NAIK, Dilip. *Internet: standardy a protokoly*. Vydání první. Praha: Computer Press, 1999. Internet. ISBN 80-722-6146-0.

[23] KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 3. aktualiz. a rozš. vyd. Praha: Computer Press, 2002. Všechny cesty k informacím. ISBN 80-722-6675-6.

[24] PETERKA, Jiří. Relační vrstva. *EArchiv: Archiv článků a přednášek Jiřího Peterky* [online]. Jiří Peterka, 2015 [cit. 2020-04-01]. Dostupné z: https://www.earchiv.cz/a92/a225c110.php3

[25] PETERKA, Jiří. Prezentační vrstva. *EArchiv: Archiv článků a přednášek Jiřího Peterky* [online]. Jiří Peterka, b.r. [cit. 2020-04-03]. Dostupné z: https://www.earchiv.cz/a92/a226c110.php3

[26] LAMMLE, Todd. *CCNA: výukový průvodce přípravou na zkoušku 640-802*. Brno: Computer Press, 2010. ISBN 978-80-251-2359-1.

[27] PETERKA, Jiří. Aplikační vrstva. *EArchiv: Archiv článků a přednášek Jiřího Peterky* [online]. Jiří Peterka, b.r. [cit. 2020-04-03]. Dostupné z: https://www.earchiv.cz/a92/a227c110.php3

[28] PETERKA, Jiří. Rodina protokolů TCP/IP. *EArchiv: Archiv článků a přednášek Jiřího Peterky* [online]. Jiří Peterka, b.r. [cit. 2020-04-04]. Dostupné z: https://www.earchiv.cz/anovinky/ai1592.php3

[29] PETERKA, Jiří. Síťový model TCP/IP. *EArchiv: Archiv článků a přednášek Jiřího Peterky* [online]. Jiří Peterka, b.r. [cit. 2020-04-07]. Dostupné z: https://www.earchiv.cz/a92/a231c110.php3

[30] Rozdělení počítačových sítí podle rozlehlosti. *Multimediální podpora předmětu Internet a jeho služby* [online]. b.r. [cit. 2020-04-11]. Dostupné z: http://ijs.8u.cz/index.php/pocitacove-site/rozdeleni-pocitacovych-siti-podle-rozlehlosti

[31] Počítačová síť. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2020-04-11]. Dostupné z: https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5

[32] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 3., aktualiz. vyd. Brno: Computer Press, 2006. Bestseller (Computer Press). ISBN 80-251-0892-9.

[33] SPORTACK, Mark A. *Směrování v sítích IP: [autorizovaný výukový průvodce : samostudium : kompletní zdroj informací o směrování a protokolech v sítích IP]*. Brno: Computer Press, 2004. Cisco systems. ISBN 80-251-0127-4.

[34] SATRAPA, Pavel. *IPv6: internetový protokol verze 6*. 4. aktualizované a rozšířené vydání. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88-168-43-0.

[35] VELTE, Toby a Anthony VELTE. *Síťové technologie Cisco: velký průvodce*. Vydání první. Brno: Computer Press, 2003. Administrace (Computer Press). ISBN 80-722-6857-0.

[36] Pasivní síťové prvky. *Internet a jeho služby* [online]. b.r. [cit. 2020-06-20]. Dostupné z: http://ijs2.8u.cz/index.php?option=com_content&view=article&id=19&Itemid=124

[37] Horizontální komunikace mezi vrstvami. In: *EArchiv: Archiv článků a přednášek Jiřího Peterky* [online]. Jiří Peterka, 2015 [cit. 2020-03-20]. Dostupné z: https://www.earchiv.cz/b05/b0500001.php3

[38] PETERKA, Jiří. Sedm vrstev ISO/OSI. In: *EArchiv: Archiv článků a přednášek Jiřího Peterky* [online]. b.r. [cit. 2020-03-22]. Dostupné z: https://www.earchiv.cz/b05/b0500001.php3

[39] Hlavička protokolu TCP. In: *Materiálovotechnologická fakulta - Materiálovotechnologická fakulta STU v Bratislave: Protokol TCP* [online]. Trnava: Materiálovotechnologická fakulta so sídlom v Trnave, 2020 [cit. 2020-03-31]. Dostupné z: http://www.uiam.mtf.stuba.sk/predmety/ps/CD-0x/9.html

[40] Hlavička protokolu UDP. In: *ČVUT - Fakulta elektrotechnická* [online]. Praha: ČVUT - Fakulta elektrotechnická, b.r. [cit. 2020-03-31]. Dostupné z: https://cw.fel.cvut.cz/b182/_media/courses/a5m33izs/x33dsp_site-1.pdf

[41] PETERKA, Jiří. Vztah relace a transportního spojení. In: *EArchiv: Archiv článků a přednášek Jiřího Peterky: Relační vrstva* [online]. Jiří Peterka, 2015 [cit. 2020-04-01]. Dostupné z: https://www.earchiv.cz/a92/a225c110.php3

[42] PETERKA, Jiří. Srovnání vrstev RM ISO/OSI a TCP/IP. In: *EArchiv: Archiv článků a přednášek Jiřího Peterky* [online]. Jiří Peterka, b.r. [cit. 2020-04-04]. Dostupné z: https://www.earchiv.cz/anovinky/ai1592.php3

[43] PETERKA, Jiří. Protokoly a vrstvy TCP/IP. In: *EArchiv: Archiv článků a přednášek Jiřího Peterky* [online]. Jiří Peterka, b.r. [cit. 2020-04-04]. Dostupné z: https://www.earchiv.cz/anovinky/ai1592.php3

[44] PETERKA, Jiří. Zjištění fyzické adresy podle IP adresy (protokol ARP). In: *EArchiv: Archiv článků a přednášek Jiřího Peterky* [online]. Jiří Peterka, b.r. [cit. 2020-04-08]. Dostupné z: https://www.earchiv.cz/a92/a235c110.php3

[45] PETERKA, Jiří. Zjištění vlastní IP adresy pro bezdiskovou stanici (protokol RARP). In: *EArchiv: Archiv článků a přednášek Jiřího Peterky* [online]. Jiří Peterka, b.r. [cit. 2020-04-08]. Dostupné z: https://www.earchiv.cz/a92/a235c110.php3