Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Analýza a optimalizace routingu a zabezpečení v prostředí lokálního internetového providera

Základy směrování k lokální síti providera

Bakalářská práce

Autor: Lukáš Urban
Studijní obor: Informační management

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové Duben 2020

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 29.4.2020 Lukáš Urban

Poděkování:

Děkuji vedoucímu bakalářské práce Mgr. Josefu Horálkovi, Ph.D. za metodické vedení práce, za pomoc a rady při zpracování této práce. Dále bych chtěl poděkovat mému dlouholetému kamarádovi, který vlastní a provozuje službu v poskytování internetu a umožnil mi přístup do jeho vnitřní sítě.

Anotace

Obsah práce se bude zabývat možnostmi připojení uživatelů k síti internet. V práci budu popisovat základní možnosti, které dnešní technologie umožňuje. Práce je rozdělena do několika základních částí. První, teoretická část práce, se zabývá otázkou práv a povinností všech lokálních poskytovatelů internetu, dále jejich možností propojitelnosti a jejich technologickými možnostmi, a na konec samotnou otázkou směrování. Všechny tyto informace jsou popsány a směrovány všem lidem bez zvláštních předchozích znalostí o fungování počítačových sítí a jejich směrování. V práce se objasňují základní pojmy a principy ze světa směrování v počítačové síti. Druhá, praktická část, simuluje na praktické ukázce, jak dochází ke směrování požadavku ve vnitřní síti poskytovatele. V závěrečné části této práce je vyhodnoceno zabezpečení na úrovni směrování a aplikování řešení na zvýšení zabezpečení na straně poskytovatele.

Annotation

Title: Analysis and optimization of routing and security in the environment of a local Internet provider

The content of this work will deal with the possibilities of connecting users to the Internet. In this work I will describe the basic possibilities that today's technology allows. The thesis is divided into several basic parts. The first, theoretical part of the thesis deals with the question of rights and obligations of all local Internet providers, their connectivity and technological possibilities and finally the question of routing. All this information is described and directed to all people without special prior knowledge of how computer networks work and how they are routed. The work explains the basic concepts and principles of the world of routing in a computer network. The second practical part simulates a practical demonstration of how the request is routed in the provider's internal network. In the final part of this thesis is evaluated security at the level of routing and application of security enhancement solutions on the provider side.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Připojení k internetu je v dnešní době již technologický standard. Jak je možné, že se na trhu služeb objevují internetoví poskytovatelé? K tomu, aby bylo možno tuto službu využívat, tak jí nejprve musí někdo poskytnout. Připojení k síti internetu může být uskutečněno právě díky poskytovatelům internetu. Podoba poskytovatele může být různá, může se jednat například o lokálního nebo celorepublikového poskytovatele. Může se lišit v mobilitě připojení na mobilní nebo pevné připojení a v podobě tarifikace dat na neomezené nebo účtované. Možností je mnoho a vždy závisí na požadavcích zákazníka, které z těchto variant zvolí.

Co všechno musí poskytovatel splnit, aby se vůbec dostal k tomu, že začne přemýšlet jak nejlépe udržovat a rozšiřovat svou síť? To je úplně ta prvotní myšlenka, na kterou se práce snaží odpovědět a zdůraznit povinnosti každého poskytovatele, které vycházejí ze zřizovacích povinností. Druhou otázkou jsou legislativní povinnosti, které vycházejí z provozu a jsou definovány zákony a vyhláškami. Třetí povinností každého poskytovatele jsou provozní povinnosti, které vyplývají z podstaty a jsou částečně definovány samotným poskytovatelem.

Pokud dojde k domluvě s poskytovatelem internetu, tak je důležité si zjistit, jak do sítě budeme přistupovat. Tedy typ připojení. Možnost typu připojení / spojení je další zásadní myšlenkou, kterou je třeba si objasnit před tím, než bude popsáno samotné směrování. Síť poskytovatele není sestavená pouze z jednoho typů připojení a spojení, ale jedná se standardně o kombinaci více typů. Jaké jsou možnosti pevných nebo komutativních připojení? Tím vším se zabývá druhá část práce.

Jak síť funguje a z čeho se skládá? Pro nejlepší pochopení, jak datová sít funguje, je princip vysvětlen na ISO/OSI modelu. ISO/OSI model je základním modelem fungování síťové komunikace. Z ISO/OSI modelu vyplývá TCP/IP protokol, který je jedním z rodiny nejznámější komunikačních protokolů a díky kterému je popsána podstata směrování a vše co směrování v síti obnáší.

Získané poznatky a informace jsou v této práci zakončené na praktické ukázce. Praktická ukázka znázorňuje, jak směrování v síti probíhá. Pro představu je

použit oficiální volně stažitelný software od společnosti MikroTik (www.mikrotik.com) WinBox 3.22.

2 Cíl práce

Cílem práce je provést analýzu stávajícího stavu sítě lokálního providera a seznámit se se základní logikou a principy, ze kterých je síťové směrování složeno. Ať už z pohledu poskytovatele ze zákonných povinností, které popisuje kapitola č. 4., tak z technických možností připojení, které jsou popsány v kapitole č. 5. Principy síťového směrování jsou popsány na ISO/OSI modelu, který je základním kamenem síťové komunikace. Proto je v práci kladen důraz na jeho pochopení a tím i pochopení TCP/IP modelu, který je na ISO/OSI modelu prezentován. Díky této struktuře bude možné porozumět samotné logice směrování v sítích a následné praktické části. V praktické části budou všechny poznatky aplikovány na názorné ukázce ve směrování napříč vnitřní sítí a současné analýze stavu provozu a zabezpečení. Zjištěné nedostatky v rámci analýzy pak budou předány poskytovateli, včetně doporučení na nápravná opatření.

3 Metodika zpracování

Bakalářská práce se soustředí na popis činnosti v rámci poskytování dat v síti. Jedná se o velice komplikovaný proces, při kterém musí být vše organizované a správně nastavené. V jiném případě by síť nefungovala korektně a data by se nedostávala ve správný čas na správné místo. V této práci jsou uplatněny všechny moje dosud nasbírané zkušenosti se správou počítačových sítí a informace, které byly získané od konkrétního poskytovatele internetu. Proces směrování je velice složitý, proto je tento proces v práci popsán nejen na teoretické úrovni, ale pro lepší představu i v praktické ukázce na funkční síti. V praktické části je cílem nejen analyzovat síť, ale i upozornit na případné nedostatky týkající se nastavení, ale také i v zabezpečení směrování.

4 Lokální internetový provider a jeho povinnosti

Hlavní podstatou internetového poskytovatele internetu je poskytnout tuto službu všem připojeným uživatelům. Žijeme v digitální době, která konektivitu k síti internet téměř předpokládá a vychází z faktu, že se většina věcí dokáže odehrávat právě zde. Internet je tedy pro dnešní dobu klasicky používané slovo spojené s informacemi, daty, zábavou nebo i sociálním prostředím. Samotná podstata internetu je založena na spojování počítačů v globálním rozměru. Nejde tedy jen o spojení zařízení v jedné ulici, ale je to celosvětová síť založená na principu spojení všech zařízení. Pojmem „internet“ by se dal vysvětlit dvěma způsoby. První pojem označuje síť jako samotnou celosvětovou síť, ke které se uživatelé připojují pomocí svých poskytovatelů internetu. Druhý pojem pak označuje samotný obsah, který je díky této síti dostupný. Tento obsah je možné nalézt, nastudovat či si ho přímo uložit na své datové uložiště. Pomocí služby internetového poskytovatele máme možnost se připojit do této veřejné světové sítě a využívat veškeré možnosti, které tato síť nabízí. Síť internet nám dokáže ulehčovat denní povinnosti, plnit zábavu, ale samozřejmě s sebou nese i skrytá nebezpečí v podobě nejrůznějších kyberzločinů. Ačkoliv je síť virtuálním prostředím, tak i zde platí pravidla, která musí všichni uživatelé dodržovat. Jinak tomu není ani v případě internetového poskytovatele, který musí splnit a dodržovat nejen všeobecná pravidla, ale i státem stanovené legislativní podmínky.

Základní povinnosti internetového providera by se daly rozdělit do tří kategorií, kde každá z kategorií se zabývá odlišnou problematikou. První kategorie (zřizovací) se zabývá povinnostmi, které musí poskytovatel splnit, aby vůbec mohl tuto službu začít nabízet – tedy zajištění licence a zápis do obchodního rejstříku. Druhá kategorie (legislativní) pohlíží na povinnosti, které jsou poskytovateli uděleny legislativou – jednoduše řečeno, co musí poskytovatel dodržovat. Do poslední kategorie se řadí povinnosti, které, poskytovateli vznikají v rámci služby provozování.

4.1 Povinnosti lokálního internetového providera

4.1.1 Zřizovací povinnosti

Poskytovatel internetu je fyzická nebo právnická osoba, která chce vykonávat nebo již vykonává činnost, kterou je podnikáním v elektronických komunikacích. Stejně jako ostatním podnikatelským oborům v České republice, tak i poskytovatelům internetu vznikají nutné legislativní povinnosti. První povinnost je pro všechny osoby zahajující podnikatelskou činnost na území ČR stejná. Je jím zápis do obchodního rejstříku dle § 42 zákona č. 304/2013 Sb. o veřejných rejstřících právnických a fyzických osob [1], který cituje, že do obchodního rejstříku se zapisují:

a) obchodní společnosti a družstva podle zákona upravujícího právní poměry obchodních společností a družstev (dále jen „obchodní korporace"),

b) fyzické osoby,

1. které jsou podnikateli, mají bydliště v České republice a požádají o zápis, a

2. uvedené v § 43, které podnikají na území České republiky, a požádají o zápis, a

c) další osoby, stanoví-li povinnost jejich zápisu tento nebo jiný zákon.

Poskytovatelem internetu proto může být jak fyzická osoba, tak i právnická osoba. Druhou legislativní povinností je dle § 13 zákona č. 127/2005 Sb. o elektronické komunikaci povinnost oznámit předem tuto skutečnost Českému telekomunikačnímu úřadu (dále ČTU). Po doložení a splnění všech obecných podmínek vydává ČTU poskytovateli osvědčení, potvrzující, že tato osoba předložila oznámení a současně fyzické osobě přidělí identifikační číslo, pokud jí dosud nebylo přiděleno.

4.1.2 Legislativní povinnosti

Z legislativního hlediska je každý poskytovatel povinen uchovávat údaje o komunikaci zprostředkované ve svých sítích dle plnění legislativní povinnosti podle § 97 odst. 3 zákona č. 127/2005 Sb. o elektronické komunikaci a vyhlášky o uchovávání, předávání a likvidaci provozních a lokalizačních údajů č. 357/2012 Sb. Dále dle § 73 odst. 7 a 8 zákona č. 127/2005 Sb. o elektronické komunikaci je poskytovatel zajišťující veřejnou komunikační síť povinen uveřejnit a oznámit úřadu typy rozhraní, která nabízí pro připojení přístrojů, a jejich technické specifikace.

- **Zákon č. 127/2005 Sb. § 97** odst. 3 zákona o elektronické komunikaci [2] přímo cituje: *Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací. Provozní a lokalizační údaje týkající se neúspěšných pokusů o volání je právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna uchovávat pouze tehdy, jsou-li tyto údaje vytvářeny nebo zpracovávány a zároveň uchovávány nebo zaznamenávány. Současně je tato právnická nebo fyzická osoba povinna zajistit, aby při plnění povinnosti podle věty první a druhé nebyl uchováván obsah zpráv a takto uchovávaný dále předáván. Právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, je na požádání povinna je bezodkladně poskytnout.*
- **Vyhláška č. 357/2012 Sb. § 2** přímo definuje rozsah uchovávání provozních a lokalizačních údajů, které musí poskytovatel u každého spojení uchovávat. Vyhláška definuje jednotlivé sítě a jejich povinnosti, lokální poskytovatel internetového připojení je definován v odstavci č. 3. Dle vyhlášky [3] se jedná o tyto údaje:

  1. typ připojení,

2. telefonní číslo nebo označení uživatele,

3. identifikátor zařízení,

4. adresa MAC zařízení uživatele služby,

5. datum a čas zahájení a ukončení připojení k internetu,

6. označení přístupového bodu u bezdrátového připojení k internetu,

7. adresa IP a číslo portu, ze kterých bylo připojení uskutečněno.

- **Zákon č. 127/2005 Sb. § 73** odst. 7 a 8 zákona o elektronické komunikaci [4] přímo cituje z odst. 7: *Podnikatel zajišťující veřejnou komunikační síť je povinen uveřejnit způsobem umožňujícím dálkový přístup a oznámit Úřadu typy rozhraní, která nabízí pro připojení přístrojů, a jejich technické specifikace. Tyto povinnosti musí splnit nejpozději 1 měsíc před tím, než budou veřejné telekomunikační služby poskytované prostřednictvím těchto typů rozhraní k dispozici. Změny technické specifikace je povinen oznámit Úřadu a uveřejnit způsobem umožňujícím dálkový přístup, a to nejpozději 3 měsíce přede dnem jejich provedení.*

  Z odst. 8: *Technické specifikace uvedené v odstavci 7 musí být natolik podrobné, aby umožňovaly konstruovat přístroje schopné využívat všechny veřejně dostupné služby elektronických komunikací, které jsou prostřednictvím příslušných rozhraní poskytovány. Technické specifikace musí obsahovat veškeré informace nezbytné k tomu, aby výrobci mohli provádět příslušné zkoušky s ohledem na technické požadavky platné pro přístroje.*

4.1.3 Provozní povinnosti

Z názvu provozní povinnosti již vyplývá, o jaké povinnosti a závazky se bude jednat. Jsou to povinnosti, které vyplývají ze samotného provozu. Všechny typy povinností se současně prolínají a jsou na sobě závislé, nejvíce se však mísí legislativní a provozní povinnosti. Rozdíl v těchto pojmech je v samotném vzniku a charakteru. Legislativní povinnosti jsou definovány zákony či vyhláškami. Provozní povinnost je částečně definována samotným poskytovatelem. Mezi základní a hlavní část patří dodržování nastavených a oboustranně odsouhlasených všeobecných

podmínek, které jsou součástí smlouvy o poskytování služeb. V těchto dokumentech se vzájemně smluvní strany zavazují k dodržování základních závazků. Tyto závazky se mohou u jednotlivých poskytovatelů lišit.

5 Typy připojení

Na začátek tohoto tématu je třeba se zabývat problematikou, která řeší základní problém a tím je samotné připojení. Dnešní „moderní“ technologie nám nabízí hned několik možností, jak je možné klienty připojit k síti a poskytovat jim službu konektivity. Volba nejlepšího řešení je vždy závislá na mnoha faktorech, které jí přímo ovlivňují.
Typ připojení lze dělit dle doby připojení následovně:

- komutované,
- pevné.

5.1 Komutované připojení

Komutované připojení není z pohledu lokálního internetového providera nijak zajímavé a ani technologicky proveditelné, protože se jedná a typ připojení, které nabízí pouze dočasné připojení. Standardní lokální provideři poskytují tzv. pevné (stálé) připojení. Principem tohoto připojení je, že se uživatel připojí k síti pouze v okamžiku, když potřebuje získat data a poté se opět odpojuje.
Mezi takové připojení patří např. vytáčená linka, ISDN nebo mobilní připojení. Vytáčená linka je dnes již minimálně využívaný typ připojení. Připojení k internetu probíhá pomocí veřejné pevné telefonní linky, která je analogová. U uživatele internetu tedy musí být umístěn analogový modem, který převádí analogový signál na digitální. Uživateli jsou následně účtovány poplatky za dobu využívání této linky, proto se toto připojení řadí do skupiny dočasných připojení. Rychlost připojení: do 56 Kb/s.
ISDN je dnes opět již minimálně využívaný typ připojení. Jedná se o tzv. nadstavbu vytáčené linky jen s tím rozdílem, že přenos probíhá přes digitální linku. I zde musí uživatel vlastnit modem, nebo ISDN kartu a platí za dobu využívání. V případě

vyšších rychlostí (cca 128 Kb/s) i dvojnásobně. Digitální síť již zajišťuje větší stabilitu sítě. Rychlost připojení: do 128 Kb/s.
Mobilní připojení je jedna z nejčastějších alternativ pevného připojení k internetu. Uživateli umožňuje připojení z libovolného místa (v závislosti na signálu mobilní sítě). Uživatel přijímá data pomocí mobilního telefonu nebo datového modemu po aktivaci datových služeb mobilního operátora. Účtování probíhá dle připojené doby či objemu přenesených dat. Mobilní připojení v České republice prošlo od svého zavedení k velkému rozvoji. Od sítí 1G (generace), kde přenosové rychlosti byly na úrovních analogových modemů, až po sítě 4G (v blízké době i sítí 5G), jejíž teoretická přenosová rychlost činí až 299.6 Mb/s.

5.2 Pevné připojení

Pevné připojení je v současnosti nejčastěji využívaným typem připojení. Uživatel je trvale připojen k síti a standardně není omezen množstvím stažených dat. Klient platí pouze pevný měsíční poplatek.
Pevné připojení rozdělujeme do dvou skupin podle způsobu připojení:

- drátové,
- bezdrátové.

5.2.1 Drátová připojení

Pronajatý datový okruh je nejčastějším způsobem drátového připojení přes takzvaný „Pronajatý datový okruh“. Pronajatý datový okruh jsou fyzické trasy poskytované specializovanou telekomunikační společností, po kterých jsou uživateli data přenášena. Uživatel si od této společnosti objednává celou přenosovou linku s požadovanou rychlostí. Tím je zvýšena stabilita a bezpečnost sítě.

DSL připojení využívá digitální kabelové telefonní rozvody a díky lepšímu využití frekvenčních pásem dosahují vysokých přenosových rychlostí. V praxi často

označováno jako xDSL, kde první zástupný symbol (x) značí technologii digitálního přenosu. Např. ADSL, IDSL nebo HDSL. Rychlost připojení: do 52 Mb/s.
V České republice je momentálně nejvíce rozšířena technologie ADSL, kde A značí slovo „asymetrické“. ADSL tedy v překladu značí Asymetric Digital Subscriber Line. Uživateli to umožňuje současně využívat telefonní a datovou linku a to díky různým frekvenčním pásmům.
Další způsob připojení nabízí připojení k síti pomocí sítě **kabelové televize**. Kabelové televize je v dnešní době také používaným typem připojení. U tohoto typu připojení jsou využívány koaxiální kabely, které vedou do rozvodné jednotky. Rozvodná jednotka se stará o obousměrnou komunikaci s uživatelem. Přenos z těchto rozvodných jednotek dále z nebo do Internetu je pak řešen po běžných datových okruzích, tedy optickými kabely nebo bezdrátovými pojítky. Rychlost připojení: do 30 Mb/s.
Nabízí se i možnost pevného drátového připojení pomocí **silových rozvodů**. Tato síť je stále ve stavu rozvoje, protože s sebou nese zatím spoustu nevyřešených komplikací. K přenosu dat využívá jako přenosovou cestu elektrické rozvody, které jsou již zavedeny a není proto definována jejich kvalita. Mezi problémy se silovými rozvody lze zařadil například elektromagnetické rušení nebo průchod přes transformátory. V ČR se toto připojení nejvíce využívá pro domácí síť. Rychlost připojení: do 200 Mb/s.

5.2.2 Bezdrátová připojení

Bezdrátové připojení je v dnešní době jednou z nevíce využívaných technologií připojení k internetu. U tohoto typu připojení může docházet k frekvenčnímu rušení nebo mohou vznikat problémy při nepříznivém počasí, nicméně kvalita připojení je vždy závislá na frekvenčním pásmu. Bezdrátová připojení se rozděluje do dvou kategorií podle funkce:

- point-to-point,
- point-to-multipoint.

Point-to-point, nebo-li spojení bod – bod, se převážně využívá pro vytváření datových cest poskytovatelů nebo datových okruhů pro firmy. Zde je nutná pouze potřeba přímé viditelnosti a dle frekvenčního pásma dostupná vzdálenost. Toto spojení pak dokáže plně nahradit funkci kabelu. Pro zvýšení kvality přenosu jsou tyto přenosy realizovány v licencovaných pásmech. Rychlost připojení: až 3 GB/s.

Point-to-multipoint lze přeložit jako víceuživatelské připojení. Jedná se o nejpoužívanější typ připojení mezi bezdrátovými poskytovateli internetu. Pro připojení nového zákazníka většinou nemusí poskytovatel instalovat nové zařízení, ale připojí jej na již stávající přístupný přípojný bod. Na straně poskytovatele dokáže jedno zařízení obsloužit více uživatelů. Přenos dat probíhá v bez licenčním pásmu 2,4Ghz, 5Ghz a 60Ghz. Rychlost připojení: do 1 GB/s.

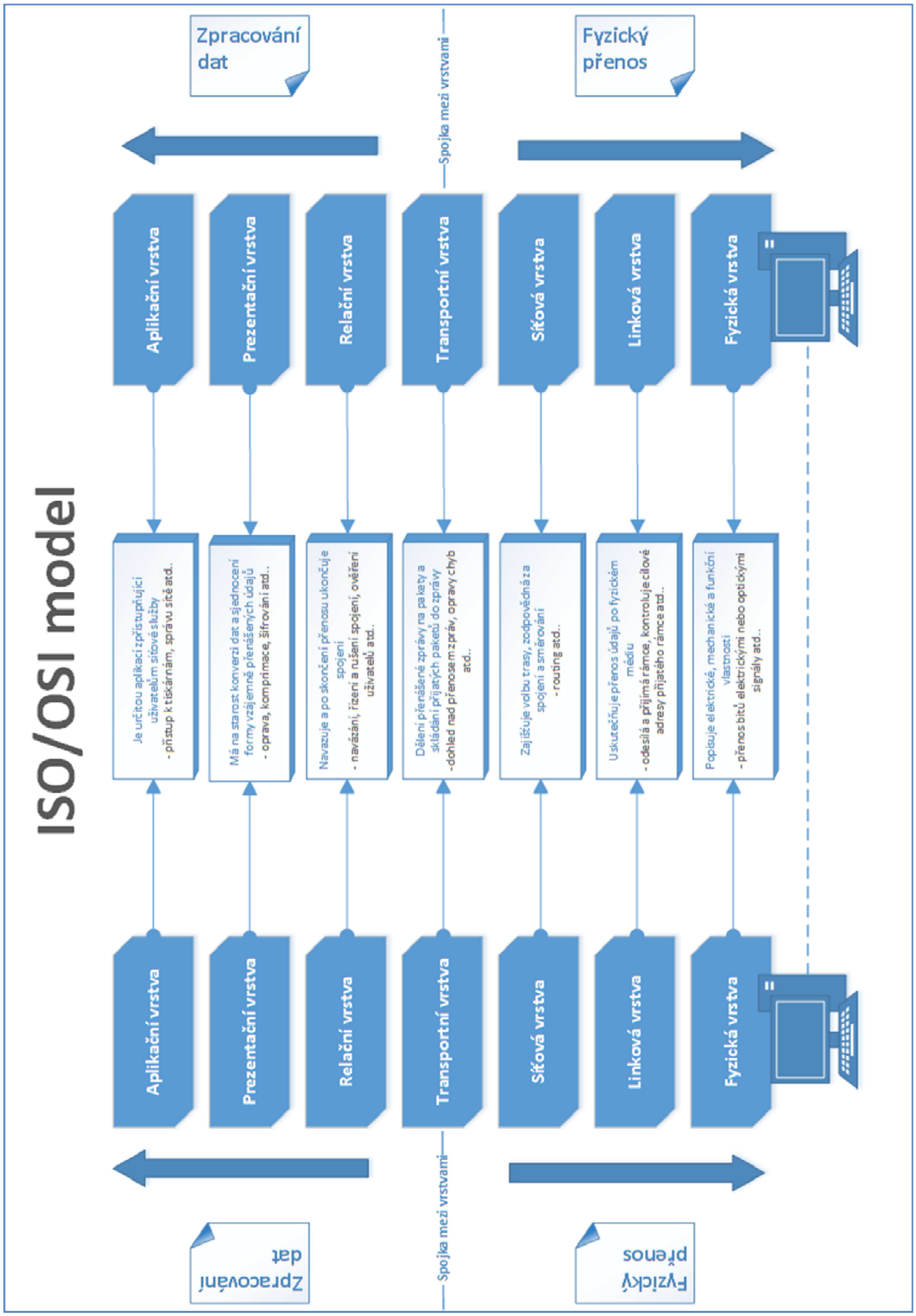
6 ISO/OSI model

Podstatou směrování je dostat informace z jednoho (startovacího) bodu sítě do druhého (cílového) bodu. K tomu, aby se tyto informace (pakety) dostaly ke svému příjemci, je potřeba stanovit pravidla pro přenos dat v sítích a mezi nimi. K tomu, aby zařízení různých výrobců byla schopna mezi sebou bezchybně komunikovat, vytvořil mezinárodní ústav pro normalizaci ISO (Internation Standards Organization) referenční model OSI (Open Systems Interconnection), který rozděluje práci v síti na 7 vzájemně spolupracujících vrstev. Dle knihy Mistrovství v počítačových sítích [5] se vrstvy dají rozdělit do dvou skupin: – *horní a dolní vrstvy.*

Horní vrstvy (5-7) souvisejí s aplikacemi a obvykle jsou implementovány v softwaru. Dolní vrstvy (1-4) souvisí s přenosem informací v síti a mohou být implementovány v hardwaru, softwaru anebo firmwaru.

Model OSI definuje obecnou strukturu, která stanovuje logické úkoly komunikace potřebné pro přesun informací mezi počítačovými systémy. Základním účelem tohoto modelu je definovat a seskupit logické funkce informačního toku. Nedefinuje tedy metody komunikace. To obstarávají komunikační protokoly, které definují pravidla, podle kterých se informace v síťových systémech vyměňují. Každá z vrstev

v modelu má své úkoly, které řeší. Dvě stejné vrstvy modelu mezi různými sítěmi či různými síťovými prvky musí umět mezi sebou spolupracovat. Princip tohoto modelu spočívá v tom, že vyšší vrstva přebírá úkol od vrstvy podřízené, zpracuje je a předá je vrstvě nadřazené. Komunikace mezi rozdílnými zařízeními pak probíhá pouze na stejné vrstvě. Práci jednotlivých vrstev, jejich uspořádání a obecný popis činností zobrazuje obrázek č. 1.



Obrázek 1 ISO/OSI model. Zdroj: vlastní zpracování

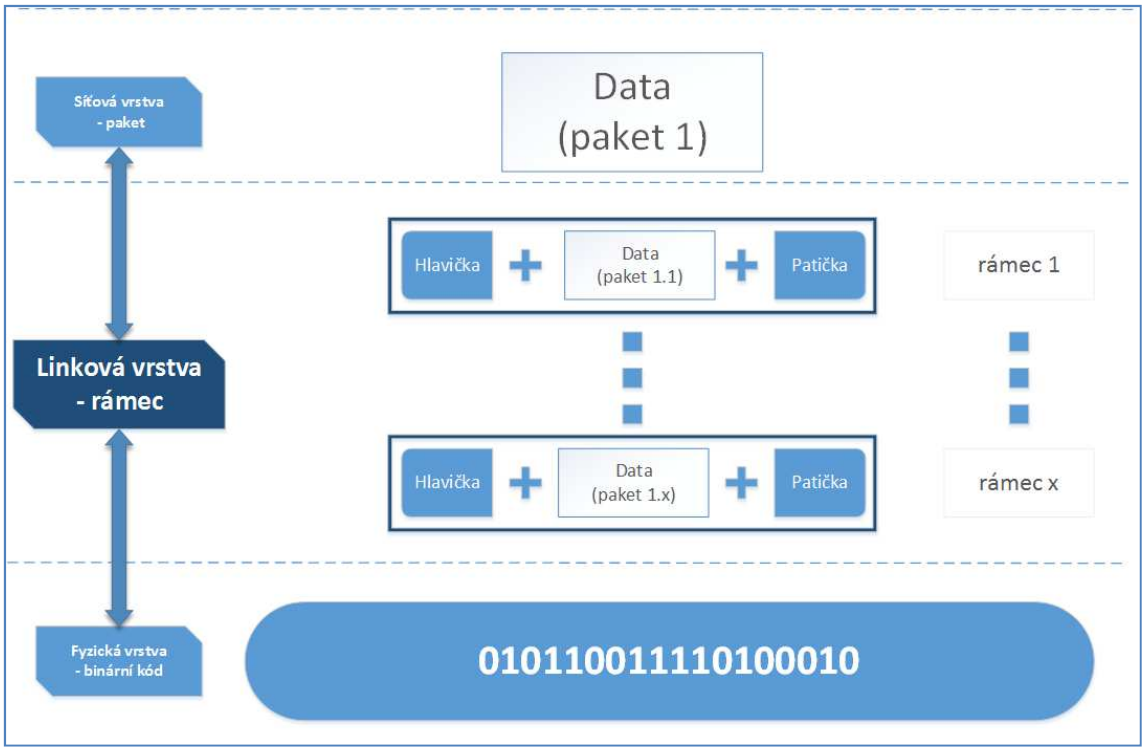
6.1 Fyzická vrstva

Fyzická vrstva je první vrstvou v ISO/OSI modelu. Z názvu je patrné, že se tato vrstva fyzicky stará o přenos dat. Podstata této vrstvy by mohla být zastoupena kapitolou číslo 5. - typy připojení, která definuje přímo zvolený typ síťového připojení. Úkolem vrstvy je pak převod binárního kódu od linkové vrstvy na signál, který se může lišit právě v závislosti na přenosovém médiu. Dnešní přenosové technologie nám tedy umožňují přenos dat pomocí drátových technologií, kde je signál přenášen elektrickými nebo optickými signály a bezdrátových technologií, kde jsou signály šířeny na základě mikrovln. Samozřejmostí vrstvy je i opačný převod ze signálu z přenosového média na binární kód.

Její přímý kontakt s přenosovým médiem jí tedy určuje tzv. hardwarovou úroveň. Na této úrovni pracují první síťové zařízení, kterými jsou huby, opakovače (repeatery), nebo samotné síťové adaptéry. K tomu, aby zařízení různých výrobců bylo schopno mezi sebou komunikovat, jsou hardwarové součásti na fyzické vrstvě definovány pomocí standartu, které stanovují elektrické a fyzické vlastnosti média, konektorů, kódování bitu nebo řídících signálů.

6.2 Linková (datová) vrstva

Na rozdíl od fyzické vrstvy, která zajišťuje přenos jednotlivých bitů mezi zařízeními, mezi kterými existuje přímé spojení, linková vrstva už přenáší větší bloky tzv. rámce. Rámec vzniká rozdělením na menší kousky a skládá se z dat převzatých z vyšší vrstvy označovaný jako paket. Úkolem vrstvy je pakety seřadit a doplnit o další potřebné informace (hlavičku a patičku), které slouží pro přenos. Tento proces se nazývá zapouzdření a v opačném případě vypouzdření.



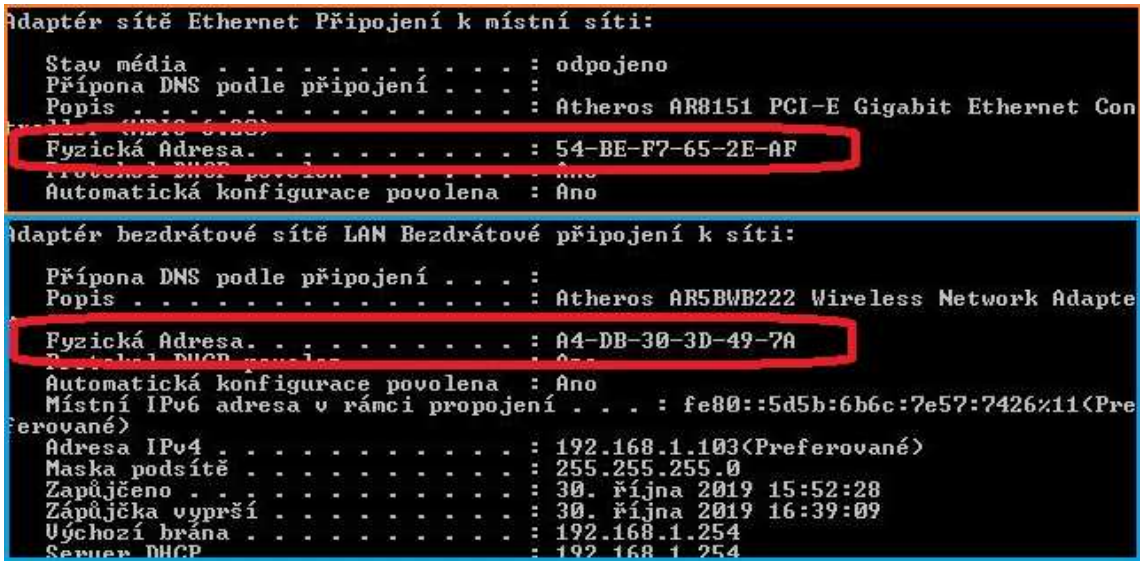
Obrázek 2 Linková vrstva - rámec. Zdroj: vlastní zpracování

Na úrovni této vrstvy jsou koncové uzly vidět pouze v dané síti – okolní sítě nevidí. Dokáže přenášet pouze data mezi dvěma uzly, které mají přímé spojení. Na této vrstvě dochází k adresaci na úrovni fyzických adres, které jsou označovány jako MAC adresy.

6.2.1 MAC adresa

MAC adresa slouží jako jednoznačný identifikátor síťového zařízení. Každé zařízení má jedinečnou adresu, která je na pevno vypálená do paměti ROM již z výroby a nelze jí standardně změnit. Jedna pracovní stanice pak může mít více adres v závislosti na počtu síťových zařízení.

MAC adresa je tvořena šesticí dvojciferných hexadecimálních čísel oddělených obvykle dvojtečkami nebo pomlčkami.

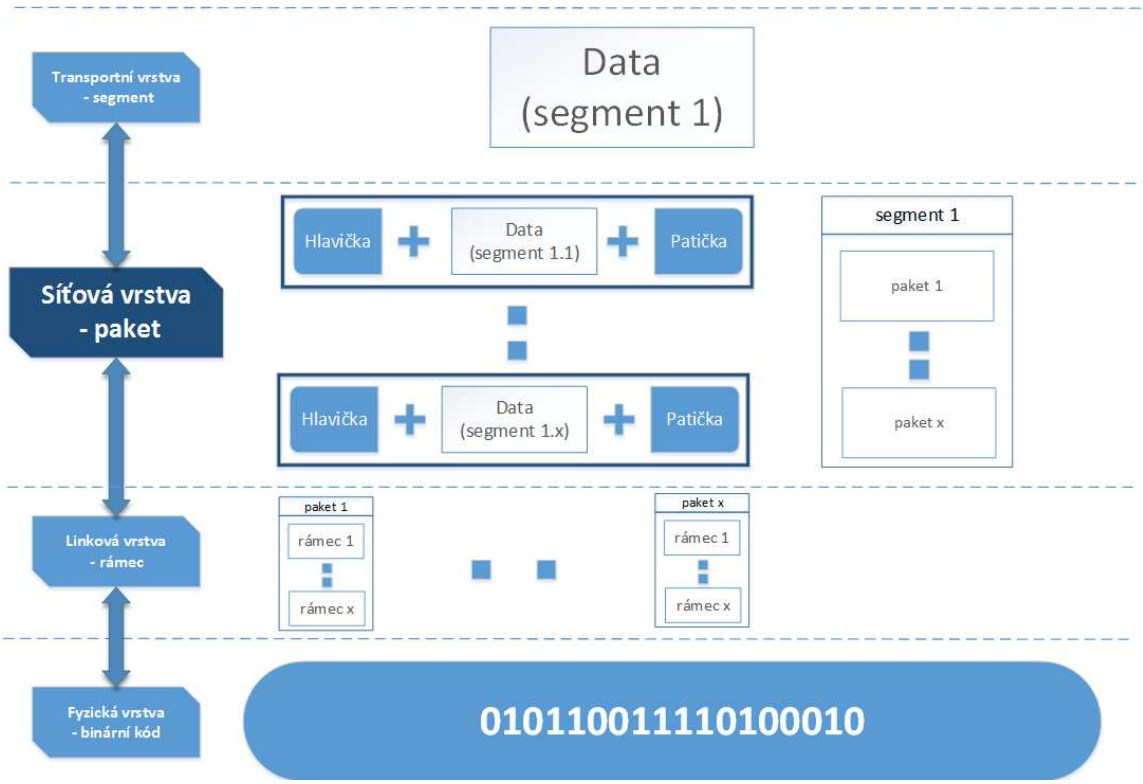


Obrázek 3 MAC adresa. Zdroj: Příkazový řádek MS Windows

Každý rámec pak nese v hlavičce MAC adresu příjemce a odesílatele. V případě, kdy stanice obdrží rámec, kontroluje adresu příjemce a v případě, že se shoduje s MAC adresou, je rámec přijat. V opačném případě je vyhodnoceno, že stanice není příjemcem a je tento rámec zahozen.

6.3 Síťová vrstva

Síťová vrstva je vrstva, která je přímo nadřazená vrstvě linkové. Na rozdíl od této vrstvy, která vidí koncové uzly jen v rámci své sítě, se síťová vrstva stará o směrování v síti a síťové adresování. Data pak již mohou putovat i za bránu své sítě do sítí sousedních. Z obrázku 4 je patrné, že na síťové vrstvě jsou přenášeny pakety. Tyto pakety jsou přenášeny napříč celou sítí ke koncovým zařízením. K tomu, aby se přenášený paket dostal ke svému příjemci, musí být na této vrstvě využity funkce, které umožní celý tento proces uskutečnit. Mezi nejdůležitější funkce tohoto procesu patří adresace, směrování, zapouzdření a naopak vypouzdření.



Obrázek 4 Síťová vrstva - paket. Zdroj: vlastní zpracování

6.3.1 Adresace

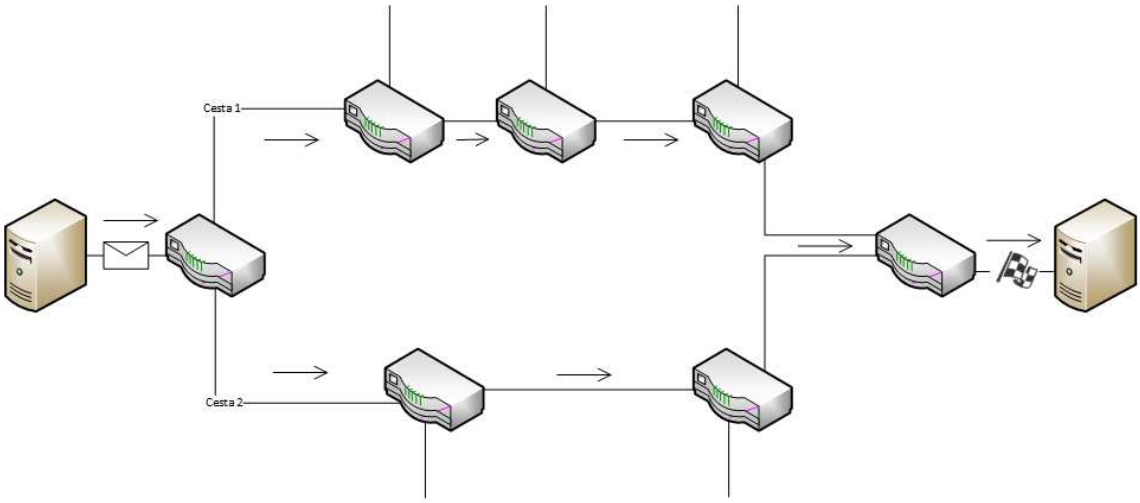
K tomu, aby jednotlivé pakety dorazily na konkrétní místo v síti, jsou koncovým zařízením v síti přidělovány jedinečné síťové adresy. Verze a podoba této adresy je definována pomocí Internet protokolu (IP, více o protokolu IP v kapitole 7.2.1), který je základním protokolem pracující na této vrstvě. Základní verzí a zatím stále ještě nejpoužívanější verzí je protokol IPv4. Z důvodu omezeného adresního prostoru (232 cca 4miliard adres) dochází v současné době k přechodu na novější protokol IPv6. Mezi další protokoly pracující na této vrstvě, patří např. ICMP.

6.3.2 Směrování

Na síťové vrstvě nejsou pakety přenášeny pouze v uzavřené síti, ale mohou být zasílány zařízením, které se nachází v sousedních sítích. Aby se paket dostal z prostředí své sítě, tak musí být nasměrován. Na každém rozhraní sítě se musí nacházet zařízení (směrovač), které tvoří pomyslnou bránu mezi jednotlivými sítěmi. Síťová brána je popsána dle knihy Počítačové sítě pro začínající správce [6]

následovně: *Kvůli mezisíťové komunikaci obsahuje IP adresa další údaj – bránu (gateway). Brána je nepovinnou částí adresy, kterou potřebujeme pouze při výměně dat mezi dvěma sítěmi. Jde opět o číselný údaj stejného formátu jako IP adresa (můžeme ji vyjádřit dvojkově, šestnáctkově i desítkově). Brána je IP adresou, na niž budou směrovány pakety v případě, že jejich adresa bude mimo rozsah vlastní sítě – budou-li posílány na adresu jiné sítě než té, z níž jsou vysílány.*

Takovýto směrovač (router) pak na základě směrovací tabulky a cílové adresy z hlavičky paketu vybírá nejlepší možnou cestu skrz síť. Pakety pak mohou být cestou k cíli směrovány přes několik směrovačů, čímž se obsah paketu nemění.



Obrázek 5 Adresace. Zdroj: vlastní zpracování

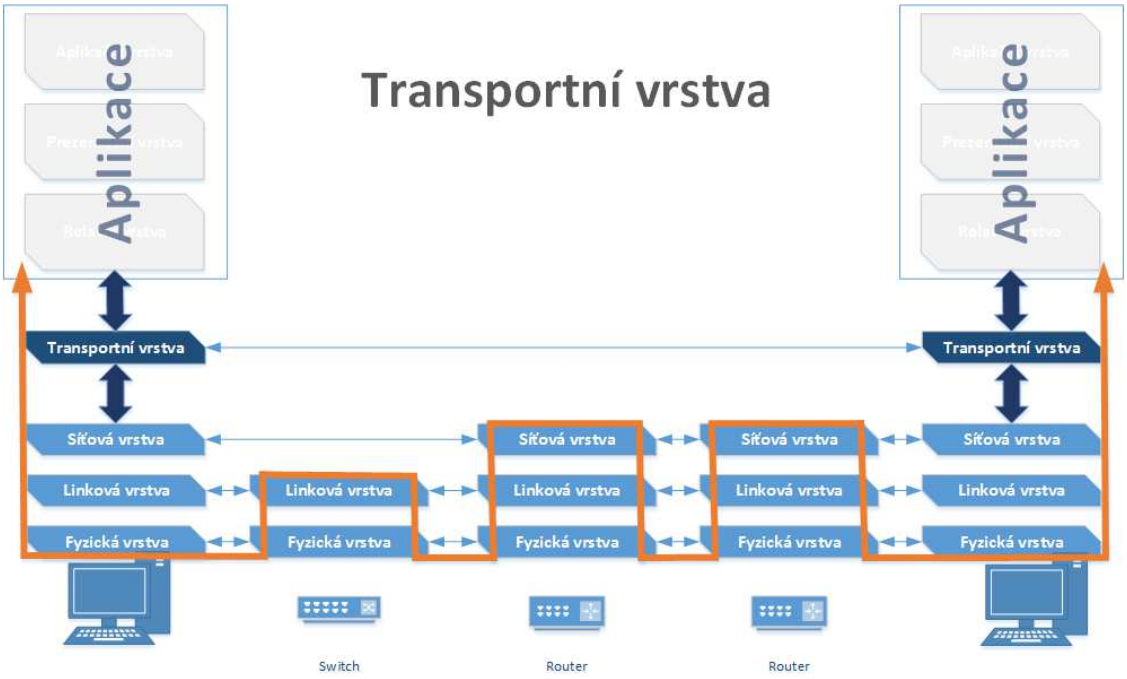
Stejně jako na linkové vrstvě, tak síťová vrstva provádí tzv. zapouzdření a vypouzdření. **Zapouzdření** (encapsulation) je proces, při kterém přebírá vrstva nižší, data od vrstvy vyšší. Rozděluje je a doplňuje je o hlavičku (případně i patičku). V případě síťové vrstvy je to tedy od vrstvy transportní, od které přijímá segmenty/datagramy. Tyto segmenty rozdělí na menší kousky, kterým přidá hlavičku a předává je linkové vrstvě.

Vypouzdření (decapsulation) je opačný proces procesu zapouzdření. Při vypouzdření přijímá vrstva vyšší data od vrstvy nižší. Na úrovni síťové vrstvy se jedná o linkovou vrstvu, od které přijímá pakety. Příslušný protokol ověřuje, zda mu

tento paket patří a v případě, že ano, tak je paketu oříznuta hlavička síťového protokolu a výsledný segment je předán transportní vrstvě. Pokud se síťová adresa neshoduje s adresou hosta, je tento paket buď zahozen, nebo dále směrován.

6.4 Transportní vrstva

Transportní vrstva je spojka, která stojí mezi vrstvami orientujícími se na přenos (fyzická, linková a síťová) a vrstvami orientujícími se na aplikace a podporu aplikací (relační, prezentační a aplikační). Mezi její hlavní úkoly patří zajišťování členění segmentů do paketů a jejich opětovné skládání. Tím je zajišťován přenos paketů mezi libovolnými dvěma uzly sítě. Transportní vrstva neřeší samotnou topologii sítě a tváří se pro ni, jako, že má každý uzel v sítí přímé spojení s kterýmkoliv jiným uzlem. Transportní vrstva se proto zabývá již jen komunikací koncových účastníků (komunikací mezí původním odesílatelem a koncovým příjemcem). Protože transportní vrstva rozděluje data do paketů a pak je opět zase skládá, umí rozpoznávat chyby a někdy je i dokonce opravovat. Jelikož při rozdělení dat na pakety jsou tyto pakety označeny číselně, dovede také odhalit nesprávné pořadí při jejich doručení a dovede je správně uspořádat. Rozpozná, kterému programu daná data patří a podle toho ho předá konkrétnímu příjemci v rámci uzlu. Transportní vrstva tedy nebývá implementována v meziuzlech (směrovačích, mostech apod.), ale až v koncových zařízeních (end-to-end). Na této vrstvě pracují dva základní protokoly TCP (více o protokolu TCP v kapitole 7.4.1) a UDP (více o protokolu UDP v kapitole 7.4.2).



Obrázek 6 Transportní vrstva. Zdroj: vlastní zpracování

6.5 Relační vrstva

Relační vrstva je nejnižší vrstva, která se orientuje na aplikace a podporu aplikací. Hlavním úkolem je navazovat, udržovat a rušit relace (doby, po kterou spolu uzly komunikují), prostřednictvím které pak probíhá komunikace mezi oběma účastníky relace. Relační vrstva nejen spravuje relace, ale řídí také dialog mezi oběma koncovými účastníky tam, kde je koordinace vyžadována. Do relační vrstvy se řadí NetBIOS nebo RPC.

6.6 Prezentační vrstva

Prezentační vrstva určuje tvar dat, v jakém jsou dostupné uživateli. To znamená, že hlavním úkolem prezentační vrstvy je přenos souborů, bezpečnost sítě a formátovací funkce. Funkcí vrstvy je tedy transformovat data do formátu, které používají aplikace. Dvě vzájemně komunikující jednotky mohou využívat rozdílných kódovacích formátů. Aby mohly společně komunikovat, musí prezentační vrstvy na obou stranách obsahovat totožné protokoly. Jedná se o pravidla pro manipulaci

s daty. Prezentační vrstva je schopna použít pro přenos dat libovolné standardy, proto má na starosti potřebné konverze z různých kódovacích znaků (ASCII, EBCDIC,...), formátu čísel, formátu struktur, polí a ukazatelů (pointerů). Vrstva se tedy zabývá jen strukturou dat, její význam je znám až vrstvě vyšší – vrstvě aplikační. Základní protokoly prezentační vrstvy jsou kryptografické protokoly TLS nebo SMB.

6.7 Aplikační vrstva

Principem vrstvy je umožnit aplikacím přístup do počítačové sítě. Slouží jako přístup k síťovým službám pro uživatelské a aplikační procesy. Zjednodušeně řečeno je pomyslnou bránou mezi aplikacemi v různých částech sítě, které si chtějí vyměňovat informace. Je tvořena množinou protokolů spolupracujících s jednotlivými aplikačními programy. Samotná vrstva aplikace neobsahuje z důvodu velkého množství různých aplikačních standardů. Aplikační vrstva obsahuje pouze aplikační jádro, které je tvořeno množstvím standardizovaných protokolů. Mezi nejzákladnější protokoly této vrstvy jsou třeba FTP, HTTP, DHCP, DNS, SMTP a mnoho dalších, které jsou popsány v kapitole 6.2. Uživatelské rozhraní proto stojí až nad touto vrstvou.

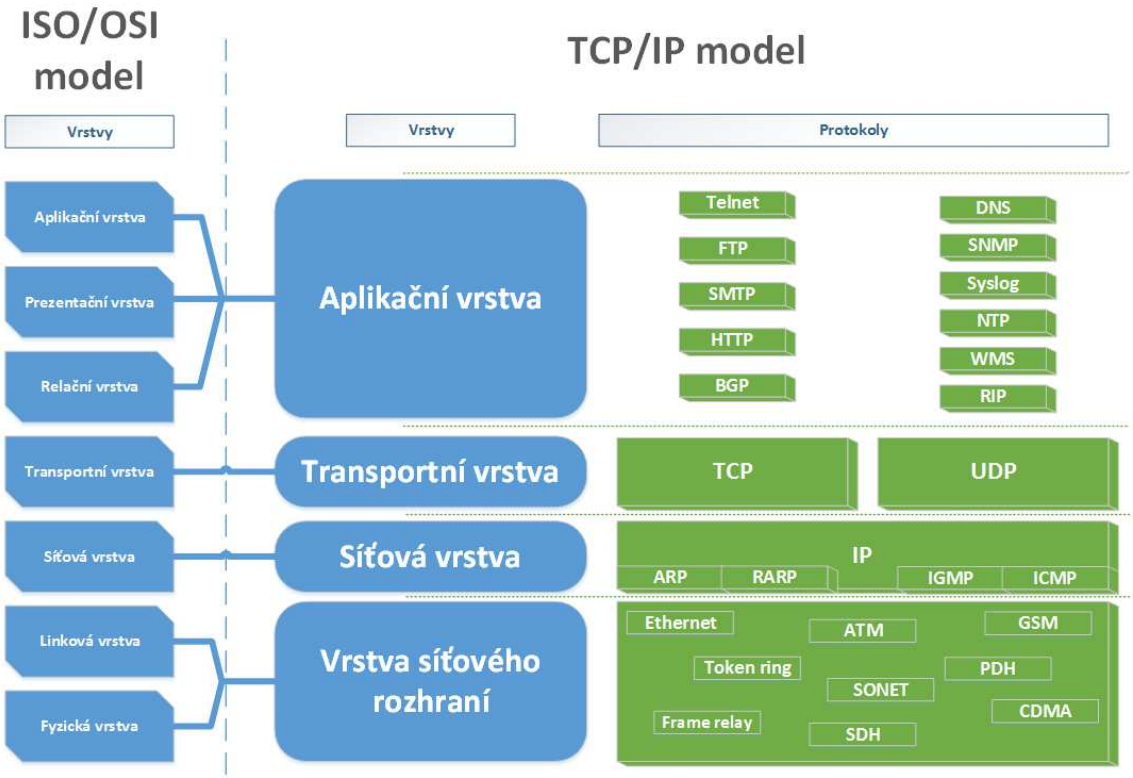
7 TCP/IP

Jak bylo zmíněno, OSI model seskupuje jak logické funkce informačního toku, tak síťové protokoly definující metody komunikace, tj. definuje komunikační pravidla, jimiž se řídí výměna dat v síti. Síťové protokoly tvoří softwarovou vrstvu, která zajišťuje formu přenosu samotných dat a stará se o spolehlivý přenos ze zdrojového na cílové zařízení určitou cestou. Od počátku elektronické komunikace vzniklo velké množství síťových protokolů, dnes se pro sítě LAN fakticky používá už jen sada protokolů TCP/IP.

Z názvu TCP/IP (Transmission Control Protocol/Internet Protocol) by se dalo vydedukovat, že se bude toto označení skládat ze dvou protokolů TCP a IP, ale není

tomu tak úplně přesně. Jedná se o celou sadu protokolů, ze které jsou TCP a IP protokoly nejznámější.

V modelu OSI se počítá a pracuje se 7 vrstvami, v modelu TCP/IP se předpokládá s rozdělením síťové komunikace pouze do čtyř vrstev. Každé vrstvě přísluší jeden či více protokolů, dva systémy pak komunikují prostřednictvím protokolů v každé z vrstev. Vrstvy jsou na sobě nezávislé a vzájemně se neovlivňují. Pokud něco řešíme na jedné vrstvě, nemusí nás zajímat, co dělají vrstvy ostatní. Největší rozdíl oproti modelu ISO/OSI je v rozdílných výchozích předpokladech a postojů tvůrců. ISO/OSI model byl konstruován a soustředěn na co možná nejvíce funkcí, což se v průběhu užívání ukázalo jako ne zcela vhodné, stejně jako v zajištění spolehlivosti. U protokolů TCP/IP se vychází z předpokladu, že zajištění spolehlivosti je problémem koncových účastníků komunikace, a mělo by tedy být řešeno až na úrovni transportní vrstvy. Na rozdíl od referenčního modelu ISO/OSI tedy TCP/IP předpokládá jednoduchou komunikační podsíť, ke které se připojují inteligentní hostitelské počítače. Další výrazná odlišnost spočívá v úvaze jak má síť fungovat. Model ISO/OSI počítá především se spojovaným přenosem, model TCP/IP naopak předpokládá nespojovaný charakter přenosu v komunikační podsíti. Je navržen tak, aby sítě byly spolehlivé, se schopností automaticky se zotavit po selhání jakéhokoli zařízení v síti.



Obrázek 7 ISO/OSI vs. TCP/IP. Zdroj: vlastní zpracování

7.1 Vrstva síťového rozhraní

Vrstva síťového rozhraní je v modelu ISO/OSI definována fyzickou a linkovou vrstvou a stejně jako v OSI modelu i zde má tato vrstva na starost fyzický přenos a přístup na přenosové médium. Přenášeny jsou standardně rámce, stejně tak jako na linkové vrstvě v OSI modelu. V modelu TCP/IP není tato vrstva blíže specifikována, neboť je specifická pro každou síť v závislosti na její implementaci. Nejčastěji využívané technologické řešení je i díky své jednoduchosti Ethernet.

Ethernet je technologie pro lokální místní sítě a používá se pro budování základu lokální počítačové sítě, která může být doplněna například wifi nebo optickou sítí.

Dle wikipedie [7]: *Ethernet je název souhrnu technologií pro počítačové sítě (LAN, MAN) z větší části standardizovaných jako IEEE 802.3, které používají kabely s kroucenou dvoulinkou, optické kabely (ve starších verzích i koaxiální kabely) pro komunikaci přenosovými rychlostmi od 1 Mbit/s po 100 Gbit/s. Sítě Ethernet realizují fyzickou a linkovou vrstvu referenčního modelu OSI, takže je možné po nich provozovat jeden nebo více protokolů síťové vrstvy.*

7.2 Internetová (síťová) vrstva

Síťová vrstva v protokolu TCI/IP má velmi podobný význam jako v modelu ISO/OSI. Z obrázku 7 je její význam na první pohled rozpoznatelný. Význam této vrstvy spočívá v zajištění směrování v síti, tj. zajištění odeslání paketu pomoci sítě a jejich směrovače.

Hlavními protokoly této vrstvy jsou IP, ARP, RARP nebo ICMP.

7.2.1 IP protokol

IP protokol patří k jednomu z nejznámějších protokolů ze sady protokolů TCI/IP, už jen kvůli samotnému označení této sady. IP protokol je založen na principu hostitelů a sítí. Hostitelem je označováno jakékoliv zařízení v síti, které je schopno odesílat a přijímat pakety. Hostitel je tedy jakékoliv zařízení v síti, které má přiřazenou IP adresu. IP adresa je jedinečná číselná hodnota, která se v síti nesmí objevovat vícekrát a označuje konkrétního hostitele. K tomu, aby spolu mohli dva hostitelé komunikovat, je zapotřebí být buď v jedné síti (sdílet společnou strukturu adres), nebo musí využívat směrovače pro směrování mezi sítěmi. IP adresa se skládá ze dvou částí: první označuje konkrétního hostitele a druhá síť, ve které se hostitel nachází.

7.2.1.1 IPv4

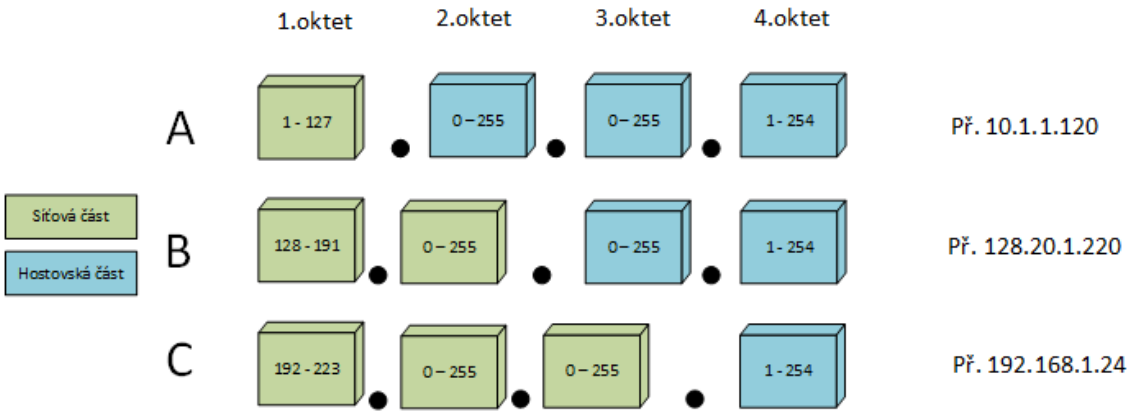
V protokolu IP verze 4 je IP adresa definována pomocí 32 bitů, tedy 4 bajtů (oktetů) vyjádřených jako čtyři desítková čísla oddělená tečkami.

Tabulka 1 IP adresa – oktety

IP adresa 16.192.80.216																
	1. oktet								2. oktet							
Velikost bitu	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Číselná hodnota	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
Zápis IP	0	0	0	1	0	0	0	0	1	1	0	0	0	0	0	0
Výpočet IP	16								. 192 (128+64)							
	3. oktet								4. oktet							
Velikost bitu	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Číselná hodnota	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
Zápis IP	0	1	0	1	0	0	0	0	1	1	0	1	1	0	0	0
Výpočet IP	80 (64+16)								. 216 (128+64+16+8)							

Zdroj: vlastní zpracování

Účel IP adresy je úplně stejný, jako účel reálné poštovní adresy a to označit konkrétního uživatele/hosta. Adresou města by se dala označit síťová část. K tomu, aby mohla být pošta doručena z města A do města B, musí dopravní prostředek vědět, jakým směrem se má k městu vydat. V síti je toto zastoupeno směrovači. Pokud dopravní prostředek zjistí, že se hostitel nenachází ve stejné síti, musí se tedy vydat do této sítě prostřednictvím směrovače. K tomu aby pak věděl, do kterého domu má být zásilka doručena, slouží hostitelská část IP adresy. Takto by bylo možné označit v reálné poštovní adrese název ulice a číslo popisné. Z IP adresy není na první pohled zřejmé, která část z adresy je síťová a která je hostitelská. K tomu, abychom byli schopni rozlišit, jak velká část IP adresy patří síti a hostiteli, dělí se IP adresy do tříd. Existují tři základní třídy IP adres: třída A, třída B a třída C.



Obrázek 8 IP adresa - třídy. Zdroj: vlastní zpracování

Adresní prostor jednoho bajtu ovšem umožňují používat až 255 čísel. Rozsah prvního oktetu jsme si dle obrázku 8 definovali pouze do hodnoty 223. Oblast 224 -239 spadá do třídy D, kde jsou adresy rezervovány pro vícesměrové vysílání, které slouží k adresování skupin specifických hostitelů. Zbývající rozsah je rezervován a slouží pro výzkumné účely. Problém ovšem nastává v momentě, kdy se zamyslíme nad počtem sítí a počtem hostů. Tato logika adresace ovšem přináší pouze omezené množství použitelných sítí a jejich hostů. Z obrázku 8 jasně vyplývá, že v třídě A, kde síti patří pouze první oktet z IP adresy, nebudeme moci vytvořit takový počet sítí jako u třídy C, kde jsou pro síť vyhrazeny oktety tři. Naopak v síti třídy A můžeme vytvořit podstatně vyšší počet hostů pro jednu síť. Původní myšlenkou bylo vytvořit strukturu, kterou by využily rozsáhlé sítě. Velkým společnostem byly přiděleny sítě třídy A, protože vyžadovaly velký adresový prostor, aby mohly vyhovět velkému počtu hostů. Počty sítí a počty hostů v jednotlivých sítí zobrazuje tabulka 2. Například v síti třídy A lze pro jednotlivou síť využívat více než 16 miliónů IP adres. Příklad takové sítě je síť 9.0.0.0, kterou má přiřazenou společnost IBM. Sítě třídy B jsou přiřazovány středně velkým společnostem a sítě třídy C malým společnostem.

Tabulka 2 IP adresa – třídy

Třída	Bitů sítě	Bitů hostů	Počet sítí	Počet hostů v každé síti
A	8	24	126	16 777 216
B	16	16	16 384	65 536
C	24	8	2 097 152	256

Zdroj: vlastní zpracování

V praxi za použití protokolu IPv4 není možné komunikovat v rámci celé sítě napřímo, ať už z fyzických nebo logických důvodů. Proto se jednotlivé sítě dále dělí na jednotlivé podsítě. Použití podsítí je metoda, díky které může být adresování logicky rozděleno do více síťových adres. Pro představu si to můžeme představit na příkladu železnice. Chceme spojit velké město železniční sítí a máme k dispozici pouze jednu kolej. Tato kolej je přetížená a nestabilní. Proto si toto město rozdělíme na několik menších částí (dle velikosti počtu uživatelů) a jednu kolej rozdělíme na více kolejí, na které budou jezdit vlaky napřímo do každé části městečka. Každá kolej tedy bude sloužit na cestu z nebo do této části města. K tomu, aby to takto mohlo fungovat, musí být tyto koleje společně s příjezdovou cestou spojeny křižovatkou. Tím nám zůstane zachována jedna příjezdová cesta (jedna síťová adresa) do města a budou obslouženy všechny části města. Pokud bychom to takto neudělali, museli bychom do každé části města přivést vlastní příjezdovou cestu do města a tím i další síťové adresy. V sítích je tato křižovatka prezentována v podobě směrovače. Takto jsme pak schopni si síť rozčlenit do několika podsítí, ve kterých bude určitý počet uživatelů. Každá síť má vyhrazené dvě adresy, které se nesmějí používat pro adresy hosta. Kniha Praktický úvod TCP/IP [8] přímo cituje: *Síťové adresy, tj. adresy, jejichž host část obsahuje samé nuly. Tyto adresy jsou využívány IP protokolem ke správnému směrování paketů mezi sítěmi. Broadcast adresy, jejichž host část obsahuje samé jedničky. Broadcast adresy se používají k hromadnému rozesílání paketů. Pošleme-li paket na broadcast adresu, dostanou ho všechny hosty v dané síti.*

Může nám pak vzniknout podsíť pro účetní oddělení, reklamační oddělení atd.. Abychom mohli podsítě efektivně využívat a nedocházelo k jejich předimenzování, využívají se masky podsítí. Významem masky je určení, která část adresy (32-bitů)

patří síťové části adresy. Jednoduše řečeno určíme, kolik bitů bude patřit pro síť, respektive podsíť. Pro lepší pochopení lze situaci znázornit na konkrétním příkladu.

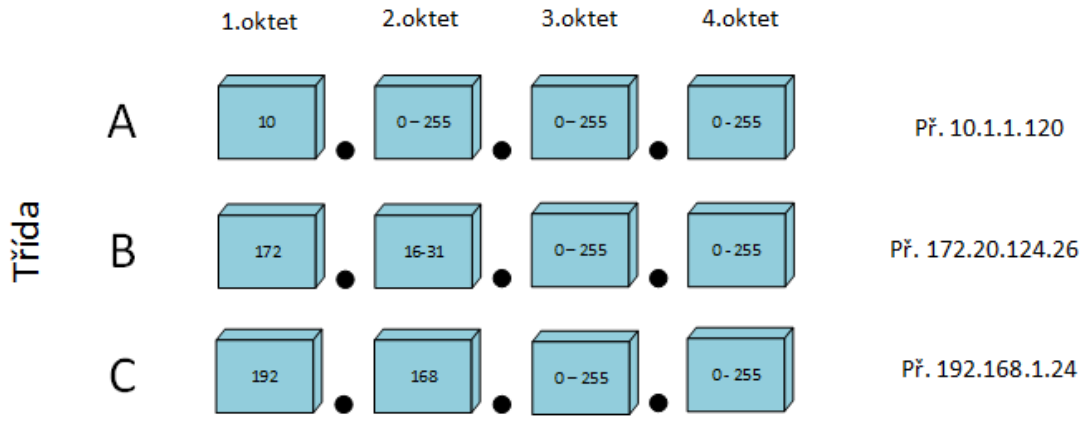
Tabulka 3 IP adresa – IPv4

IP adresa	**168.100.32.1**
binární zápis IP adresy	10101000.01100100.00100000.00000001
třída adresy	B
Maska	/16 = 255.255.0.0
binární zápis masky	11111111.11111111.00000000.00000000
IP adresa sítě	168.100.0.0
Počet síťových bitů	16
adresa síťové části	168.100.
Počet hostitelských bitů	16
adresa hostitele	.32.1
maska podsítě	/20 = 255.255.240.0
binární zápis masky podsítě	11111111.11111111.11110000.00000000
část adresy pro podsítě	10101000.01100100.**XXXX**xxxx.xxxxxxxx
část adresy pro uživatele podsítě	10101000.01100100.xxxx**XXXX.XXXXXXXX**

Zdroj: vlastní zpracování

Máme přidělenou IP adresu 168.100.32.1. Je zřejmé, že se jedná o třídu B. Pro třídu adresy B platí, že maska sítě je 16 bitů. Z této masky určíme adresu sítě (prvních 16 bitů adresy) = 168.100.0.0. Pokud si zvolíme masku podsítě 255.255.240.0 (20 bitů), pak 17, 18, 19, 20-ty bit bude sloužit pro tvorbu podsíti. Počet podsítí tedy bude 23 = 8 podsítí, pro uživatele v každé podsíti potom zbývá 12 bitů (více než 4000 IP adres).

Z důvodu omezeného adresního prostoru, se kterým se v dnešní době celosvětová síť potýká, byly zřízeny tzv. privátní adresy. Privátní adresa je taková adresa, která se může v síti vyskytovat vícekrát. Tyto síťové uzly jsou ovšem pro většinu dalších uzlů nedostupné. Dostupné jsou pouze omezenému okruhu dalších uzlů. Nejčastěji se s těmito sítěmi můžeme setkat právě v prostředí lokálního internetového providera. Poskytovatel si může zvolit, jaké adresy bude v rámci své sítě klientům přidělovat. Tyto uzly jsou pak z pohledu veřejné sítě neviditelné. Komunikace s vnějším internetovým světem probíhá nepřímo na základě různých mechanismů, jako např. pomocí NAT. Každý připojený uživatel pak nemusí mít nutně veřejnou IP adresu. V každé třídě adres byl vyčleněn adresní prostor pro tyto adresy, viz obrázek 9.



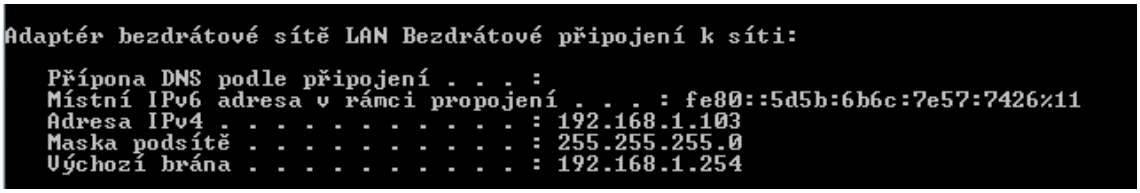
Obrázek 9 Neveřejné IP adresy. Zdroj: vlastní zpracování

Tyto privátní adresy poskytovatelé internetu sice mají ve směrovacích tabulkách, ale nepropagují je ven ze sítě. Pro použití v Internetu jsou tedy nepoužitelné. Používají se ovšem i další intervaly využívané pro speciální účely, které popisuje kniha Velký průvodce protokoly TCP/IP a systémem DNS [9]:

- *169.254.0.0/16:Blok adres pro výhradně lokální komunikaci mezi počítači. Tyto adresy využívá např. Microsoft, když se počítači žádným jiným způsobem nepodaří získat IP adresu (ani např. přes DHCP)*

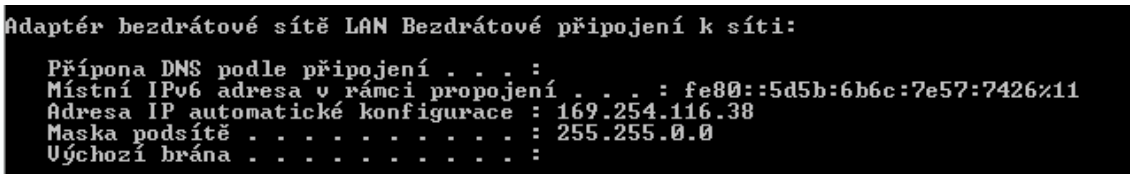
- *192.0.2.0/24: Blok přiřazený jako TEST-NET pro použití v dokumentaci a příkladech. Tyto adresy se nesmí objevit na Internetu*
- *198.18.0.0/15: Blok pro použití v testech výkonnosti (benchmark tests) – viz též RFC - 2544*

Příklad: V domácí síti je používáno dynamické přidělování IP adres, o které se stará domácí wifi router. Na wifi routeru je nastavený DHCP server pro dynamické přidělování IP adres o rozsahu 192.168.1.100 – 192.168.1.150. Za normálních okolností nám po připojení router přidělí IP adresu z tohoto rozsahu.



Obrázek 10 IP adresa. Zdroj: Příkazový řádek MS Windows

V případě, kdy se nepodaří tuto adresu získat, je automaticky nastavena tato speciální IP, obrázek 11.



Obrázek 11 Nepřidělená IP adresa. Zdroj: Příkazový řádek MS Windows

7.2.1.2 IPv6

Protokol IPv6 vznikl z důvodu nedostatku volného adresního prostoru, se kterým jsme se dnes u protokolu IPv4 setkávali. Dle zdroje Wikipedie IPv4 umožňuje využívat přibližně 4 miliardy IP adres, které mohou být v síti přiděleny. Naproti tomu u IPv6 je to 2128 IP adres, což je 5×1028 pro každého dnes žijícího člověka. V protokolu IPv6 došlo ke změně IP adresy, která již není 32 bitové číslo, ale její

délka se protáhla do 128 bitové podoby. To s sebou nese větší adresní prostor. Problém je ovšem s plošným nasazením, protože není technicky možné provést změnu ze dne na den. Z uvedeného důvod se dnes využívají pro komunikaci mezi protokoly různé translátory (překladače) nebo tunely.
IPv6 přináší spousty změn, které není nutné představovat, neboť je aktuálně v prostředí internetu stále nejčastěji používán protokol IPv4. Více informací o protokolu IPv6 lze nalézt na internetové stránce https://www.ipv6.cz/

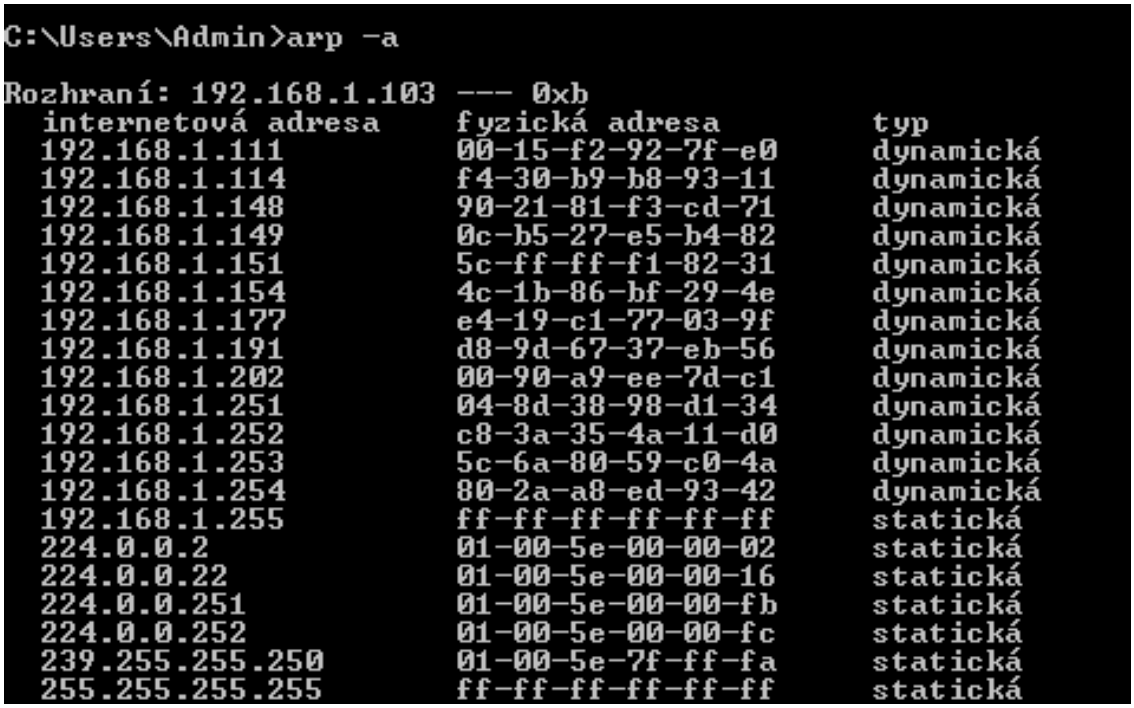
7.2.2 Protokol ICMP

ICMP protokol je úzce svázán s protokolem IP. Svým způsobem IP protokol doplňuje a to o velice důležitou službu. IP protokol poskytuje nespojovou službu. Nespojová služba znamená, že odesílatel nedostává zpětnou vazbu. Pokud by cestou nastala chyba, odesílatel by se za normálních okolností o této chybě nedozvěděl. Přesně k tomuto účelu je k IP protokolu přidružen ICMP protokol, který tuto službu zajišťuje. ICMP zprávy jsou pak generovány přímo do IP datagramu a to buď po cestě směrovači či koncovým zařízením. ICMP zpráva může nabývat různých charakterů. Jedním z druhů zpráv jsou zprávy chybové. Tento druh zprávy může vzniknout například v případě nedoručitelnosti datagramu ať už z důvodu neznámé či nedosažitelné sítě či uzlu, nebo jiných podobných chyb vedoucích k nemožnosti doručení. Dalším druhem jsou zprávy diagnostické a informativní. Diagnostické zprávy mají dotazovací význam, díky kterému je možné se dotazovat na dostupnost uzlu v síti. Je vysílána zpráva s dotazem a očekává se odpověď. Na tomto principu pracuje třeba příkaz PING, který vysílá zprávu a čeká, zda dostane odpověď. Na základě toho vyhodnotí, zda je cílová stanice dosažitelná a jak dlouho mu to trvá. Tento příkaz budeme následně využívat v praktické části. Dalším důležitým příkazem pracujících na principu diagnostických zpráv je příkaz traceroute. Tento příkaz není ovšem založen pouze na diagnostických zprávách, ale vytváří i zprávy chybové. Účelem tohoto příkazu je analýza sítě a určení trasy k cíli. Všesměrově jsou k cíli vyslány zprávy, které mají omezenou životnost. Životnost je označována jako TTL (Time-To-Live), kde s každým předáním směrovače je tato hodnota snížena

o jednu do doby, dokud není v cíli, nebo její hodnota není rovna nule. V případě nuly směrovač pakety zahazuje a zasílá chybovou ICMP zprávu odesílateli.

7.2.3 Protokol ARP

Z popisu funkcí jednotlivých vrstev OSI modelu je zřejmé, že vrstvy pro fyzický přenos balí nebo dělí data do příslušných segmentů, paketů nebo rámců. V případě zasílání dat do jiné sítě, je nutné znát adresu příjemce a znát IP adresu příjemce a znát IP adresu odesílatele. Jelikož jsou tyto pakety předávaný nižší vrstvě, která balí data do linkových rámců, potřebujeme znát i linkovou adresu. V případě ethernetového rámce se jedná o již zmiňovanou MAC adresu. K tomu, aby byla tato adresa zjištěna, slouží protokol ARP. ARP do LAN vysílá broadcastový paket, který je zasílán na všechny uživatele sítě s dotazem o nalezení MAC adresy stanice s danou IP adresou. Vlastník této IP adresy odesílateli odpovídá prostřednictvím MAC adresy. Ostatní uživatele tuto žádost ignorují. Aby nebyl tento proces neustále opakován, je adresa ukládána do mezipaměti a při další komunikaci již spolu zařízení komunikují napřímo. Všechny takto zjištěné záznamy jsou v mezipaměti uchovávány po určitou dobu. Po uplynutí této doby je položka z tohoto seznamu odstraněna. Pokud byla položka již jednou z mezipaměti odstraněna, musí být k zjištění opět spuštěn celý proces.



Obrázek 12 ARP - výpis. Zdroj: Příkazový řádek MS Windows

7.2.4 Protokol RARP

Reverzní ARP protokol se dá označit jako protiklad k protokolu ARP. Zjišťuje na základě fyzické adresy adresu síťovou. Pokud se nad tímto tvrzením více zamyslíme, začneme pochybovat o jeho smyslu. Nicméně v případě bezdiskové pracovní stanice smysl nalézáme. Bezdisková pracovní stanice zná při startu systému pouze svou fyzickou adresu, která je uložena v paměti ROM přímo od výrobce. A aby znala svou IP adresu, tak vysílá oběžník s dotazem, jakou má IP adresu. Když je na LAN RARP server, IP adresu jí přidělí a zašle jí stanici jako odpověď.

7.2.5 Protokol IGMP

IGMP protokol je dalším protokolem, který patří k IP protokolu jako služební protokol. Pakety protokolu IGMP jsou stejně jako pakety protokolu ICMP baleny přímo do IP datagramů. Funkce tohoto protokolu je multicastová. To znamená, že má za úkol šířit tzv. oběžníky v síti. Na síti LAN je definována skupina členů

oběžníku, jejichž seznam udržují multicastové routery. V případě, že se nějaká stanice přihlásí do této skupiny, tak začne router daný oběžník na LAN šířit do doby, než skupinu opustí poslední člen.

7.2.6 Autonomní systém

Pojem podsítě jsme si vysvětlili v jednom z předešlých odstavců. K tomu, abychom byli schopni pochopit, jak dochází ke směrování, je třeba si osvojit pojem autonomní systém. Samotný internet se skládá z celků, které mezi sebou komunikují a vyměňují si informace. Tyto celky by se daly prezentovat jako jednotliví poskytovatelé internetu. IP diagramy poskytovatelé dopravují buď v rámci své sítě, mezi sebou, nebo slouží pouze jako transit, kde IP diagramy pouze přes poskytovatele cestují. Tyto celky se pak z hlediska dopravy IP diagramů označují právě jako autonomní systémy. Každý poskytoval pak má přidělen jeden nebo více autonomních systému, které spravuje. Každý poskytovatel má přidělený interval IP adres, které přiděluje buď sám sobě, anebo svým zákazníkům. Zákazníci poskytovatelů se pak nacházejí v jednom autonomním systému. K čemu to je dobré? Intervaly celého poskytovatele je možné agregovat do jedné adresy označované jako supersíť. Pokud by routery musely držet všechny adresy ve směrovací tabulce, tak by tabulka musela být velice rozsáhlá a orientace v ní by byla složitá. Takto může být pro router celý interval interpretován jedinou adresou.

Př. Je-li přidělen interval adres 45.187.128.0 – 45.187.192.0, je celý tento interval agregován na adresu supersítě 45.187.128.0 / 17.

Při trasování prochází IP diagramy různými autonomními systémy, které jsou označovány ASxxxx. Např. IP adresa routeru UPC 213.192.0.0/19, přes který prochází dotaz na http stránky google.com, je v autonomním systému AS6830, který se nachází v destinaci RIPE (Evropa).

```
role:         Sloane Park Hostmaster Role
address:      UPC Ceska Republika, s.r.o.
address:      Zavisova 502/5
address:      Praha
address:      140 00
address:      Czech Republic
phone:        +420 261107111
fax-no:       +420 261107100
abuse-mailbox:  abuse@sloane.cz
remarks:      trouble: hostmaster@sloane.cz
admin-c:      MK23104-RIPE
tech-c:       JG2186-RIPE
tech-c:       JS14570-RIPE
tech-c:       JP8591-RIPE
nic-hdl:      SPHR1-RIPE
mnt-by:       SLOANE-MNT
mnt-by:       DKI-MNT
created:      2003-07-23T18:29:40Z
last-modified:  2018-09-19T07:04:06Z
source:       RIPE # Filtered

% Information related to '213.192.0.0/19AS6830'

route:        213.192.0.0/19
descr:        UPC Czech
origin:       AS6830
mnt-by:       AS6830-MNT
created:      2013-04-16T11:21:58Z
last-modified:  2013-04-16T11:21:58Z
source:       RIPE
```

Obrázek 13 Autonomní systém - výpis. Zdroj: vlastní zpracování

7.3 IP routing

Pod pojmem IP routing se schovává jednoduše znějící, avšak dost složitý proces směrování IP datagramů. Síť Internet se skládá z velkého množství routerů, které se s každým požadavkem musí rozhodovat, kam tyto jednotlivé datagramy předají. Možnosti jsou tři. Buď nasměrují datagramy přímo k příjemci, kterého ho má na dosah, nebo na sousedící router, který bude datagramy směrovat dále až ke svému cíli. Takovéto předávky mezi routery se pak nazývá termínem „HOP“. Na jedné cestě mohou IP datagramy zdolávat velké množství takovýchto „hopů“ než se dostanou na místo určení. Podstata směrování ovšem stojí v tom, jak se směrovače rozhodují, kam IP datagram předají. K tomu směrovači slouží tzv. směrovací tabulka, kterou si buď přímo udržuje směrovač, nebo jí má pevně

nadefinovanou od správce směrovače. Pro jednoduchou představu si tento proces můžeme představit na příkladu z praxe. Máme depo na třídění balíků nějakého balíkového dopravce. Na depu jedou na páse balíky (datagramy), které jsou skládaný do jednotlivých boxů, které pak putují jedním směrem (třeba do jiného města, do kterého vede přímé balíkové spojení). Obsluha na páse v Praze si přečte číslo směrovací na balíku a podle čísla směrovacího ho předá do boxu, který je odvezen konkrétním směrem do konkrétního města. Podle směrovacího čísla je zřejmé, že poštovní směrovací číslo **500** 03 patří Hradci Králové, a tak bude naloženo na auto, které pojede na depo v Hradci Králové. V Hradci králové je na depu balík znovu vyložen a poslán na pás na zatřídění. Obsluha pásu se znovu podívá na poštovní směrovací číslo a ví, že poštovní směrovací číslo **500 03** patří Hradci Králové na Slezském předměstí, proto balík předá autu, které bude rozvážet přímo na Slezském předměstí v Hradci Králové. Toto auto pak díky ulici a čísla domu doručí balík určenému příjemci. Princip směrování je stejný – jen místo obsluhy je směrovač, který používá směrovací tabulku a místo poštovního směrovacího čísla jsou IP adresy. Slezské předměstí pak pro nás už znamená LAN síť, ulice může být definována jako podsíť a číslo popisné jako konkrétní MAC adresa. Po cestě z Prahy v našem příkladu prošel balík přes dvě depa, podobně na tom jsou i datagramy, které takto procházejí přes směrovače.

7.3.1 Směrovací tabulka

```
IPv4 Směrovací tabulka
===========================================================================
Aktivní směrování:
         Cíl v síti   Síťová maska          Brána       Rozhraní Metrika
          0.0.0.0          0.0.0.0    192.168.1.254    192.168.1.103     20
        127.0.0.0        255.0.0.0         Propojené        127.0.0.1    306
        127.0.0.1  255.255.255.255         Propojené        127.0.0.1    306
  127.255.255.255  255.255.255.255         Propojené        127.0.0.1    306
      192.168.1.0    255.255.255.0         Propojené    192.168.1.103    276
    192.168.1.103  255.255.255.255         Propojené    192.168.1.103    276
    192.168.1.255  255.255.255.255         Propojené    192.168.1.103    276
        224.0.0.0        240.0.0.0         Propojené        127.0.0.1    306
        224.0.0.0        240.0.0.0         Propojené    192.168.1.103    276
  255.255.255.255  255.255.255.255         Propojené        127.0.0.1    306
  255.255.255.255  255.255.255.255         Propojené    192.168.1.103    276
===========================================================================
```

Obrázek 14 Směrovací tabulka - PC. Zdroj: Příkazový řádek MS Windows

Směrovací tabulka není záležitostí pouze routerů, ale i pracovních stanic. Směrovací tabulka slouží zařízení k tomu, aby byl schopen se orientovat v topologii sítě. Jednoduše řečeno, aby věděl, co se kolem něho nachází, anebo případně jakou cestou se k cíli dostat. Směrovací tabulku si počítač i router plní hned po startu a průběžně při jeho běhu. Dle knihy Počítačové sítě: nepostradatelná příručka k pochopení síťové teorie, implementace a vnitřních funkcí [10] může být směrování nastaveno staticky nebo dynamicky. *Statické směrování vyžaduje, aby administrátor manuálně vložil do směrovací tabulky IP adresy, které definují síťové trasy. Dynamické směrování používá protokoly k vytváření a změnám směrovací tabulky automaticky. Tyto protokoly dovolují směrovačům na síti, aby vzájemně komunikovaly a vyměňovaly si informace ze svých směrovacích tabulek.*

Metod k plnění směrovacích tabulek je tedy hned několik:

- staticky – ruční plnění pomocí příkazu,
- dynamicky – za pomocí směrovacích protokolů nebo např. ICMP zpráv.

Směrovací protokol pak obsahuje:

- cíl v síti, nebo jeho směr, za kterým se cíl může nacházet,
- síťovou masku,
- bránu, označovanou pojmem "Next Hop", tedy adresu nejbližšího routeru, přes který se bude IP datagram dopravovat,
- rozhraní dle daného systému nebo adresa síťového rozhraní, která bude použita pro předání IP datagramu,
- metriku neboli cenu, za kterou se IP datagram dostane do svého cíle – čím menší, tím lepší.

Použití směrovací tabulky

Směrovač stojí před rozhodnutím, kam má datagram poslat, proto se podívá do směrovací tabulky a začne ji postupně procházet. Princip je jednoduchý. Vezme adresu příjemce a vynásobí jí postupně se síťovou maskou v tabulce (druhý sloupec

na obrázku 14). Každý takovýto výpočet pak porovná s cílovou adresou a v případě, že najde shodu nebo dokonce více shod, kde by rozhodující ve volbě byla metrika, pošle datagram nalezeným směrem. Pokud ovšem shodu nenajde, zasílá datagram na defaultovou adresu, což je adresa 0.0.0.0 (první řádek na obrázku 14). K tomu, aby byla směrovací tabulka dynamicky plněna, používají směrovače směrovací protokoly, které tuto práci zajišťují.

7.3.2 Směrovací protokol

Dle knihy Počítačové sítě bez předchozích znalostí [11] je definice důležitosti popsána takto: *Směrovací protokoly pomáhají směrovačům nejen vůbec se o cestách dozvědět, ale také zjistit tu nejlepší cestu do cíle z několika možných. To znamená, že směrovač zjistí všechny možné cesty do cíle a poté z nich vybere tu nejlepší.*

Jedním ze základních směrovacích protokolů je protokol RIP. Dle knihy CCNA: výukový průvodce přípravou na zkoušku 640-802 [12] je RIP protokol definován takto: *Protokol RIP (Routing Information Protocol) je typickým příkladem směrovacího protokolu s vektorem vzdáleností. Protokol RIP odesílá všem aktivním rozhraním každých 30 sekund kompletní směrovací tabulku. Protokol RIP zjišťuje nejlepší cestu do vzdálené sítě výhradně pomocí počtu přeskoků. Má však standardně nastaven maximální povolený počet přeskoků na hodnotu 15, takže se cíl vzdálený 16 přeskoků považuje za nedosažitelný. Protokol RIP dobře funguje v malých sítích, ale není efektivní ve velkých sítích s pomalými spoji WAN ani v sítích s velkým počtem nainstalovaných směrovačů.*

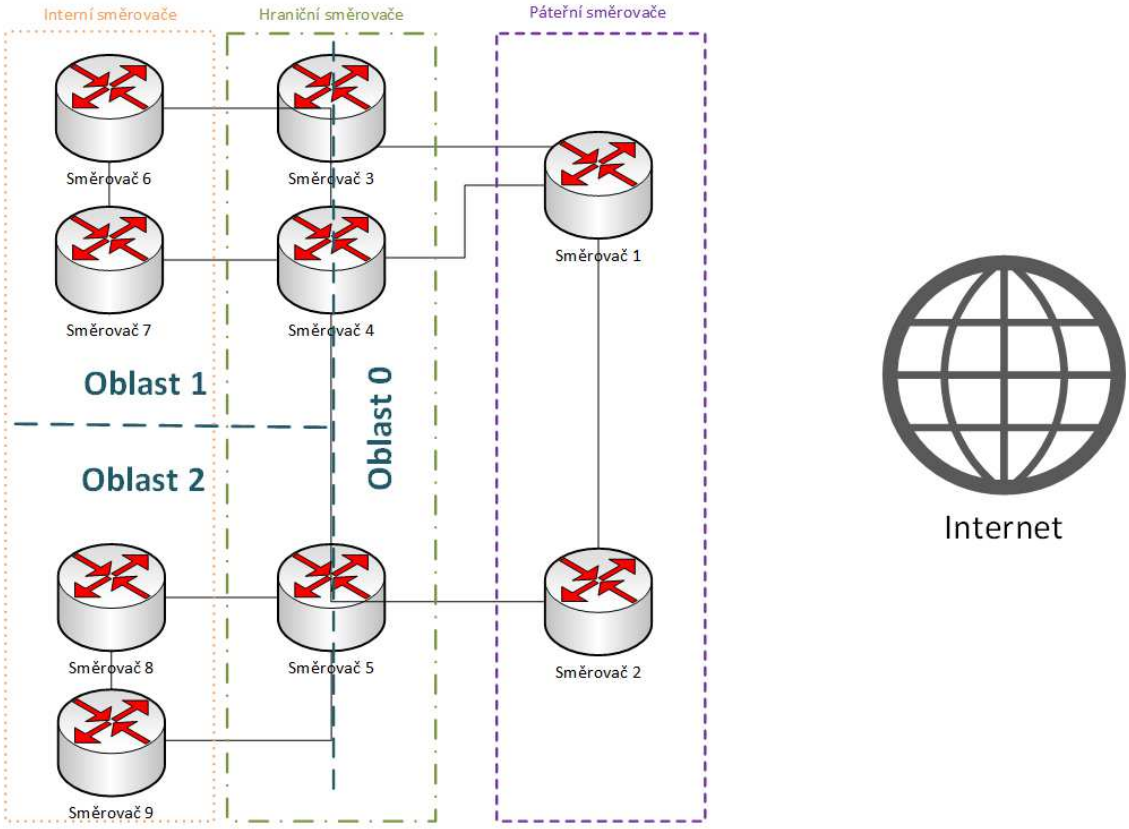
Protokol RIP verze 1 používá pouze třídní směrování, což znamená, že všechna zařízení v síti musí používat stejnou masku podsítě. Tato verze protokolu RIP totiž v rámci aktualizací neodesílá informace o masce podsítě. Protokol RIP verze 2 poskytuje funkci, která se označuje jako směrování podle prefixu (prefix routing) a odesílá s aktualizacemi tras i údaje o masce podsítě. Tato funkce se nazývá beztřídní směrování.

Mezi další z nejzákladnějších směrovacích protokolů řadíme protokol OSPF. OSPF v českém překladu znamená otevřený protokol pro nejkratší cesty. Při směrování byla zprvu použitá základní myšlenka, která nejkratší cestou definovala cestu s nejmenším počtem skoků (HOPů). Ale co když byla vybrána cesta se zhoršeným stavem linky? Tento směrovací protokol proto pracuje i se stavem linky. Tato funkcionalita mu umožňuje rychle detekovat veškeré změny v topologii autonomního systému. Výpočet je dle knihy Směrování v sítích IP [13] definován takto:

- *pro každé rozhraní OSPF se dá využít implicitní hodnota, která není citlivá vůči šířce pásma,*
- *náklady na jednotlivá rozhraní směrovačů dokáže protokol OSPF vypočítat automaticky.*

Bez ohledu na konkrétní použitou metodu se náklady v určité cestě vypočítávají vždy jako součet nákladů na všechna rozhraní podél této cesty.

Princip v síti je pak následující: všechny routery, které mají zapnutý a nastavený tento protokol, si pak v síti neustále vyměňují informace a udržují si tak identickou databázi, která sleduje stav linek v síti. Součástí databáze je samozřejmě informace o použitelných rozhraních, okolních sousedech a samotném stavu linek. Routery v síti pak přímo rozesílají všem sousedům v oblasti tyto informace, na základě kterých si každý router aktualizuje obraz aktuálního stavu sítě a jeho linek. Proces, při kterém dochází k výměně informací, má zavádějící název – záplava.
K tomu, aby bylo možné vyhovět všem zásadním požadavkům, které jsou dobrá škálovatelnost sítě a krátká doba konvergence, rozděluje se síť do menších částí. Menší části se následně označují jako oblasti. Tyto oblasti jsou identifikovány jednoznačným číslem, které má router ve svém nastavení. Když mají routery stejná čísla, patří pak logicky do jedné takové oblasti. Oblasti by měly být tvořeny tak, aby mezi nimi vznikaly smysluplné hranice, které by minimalizovaly provoz na síti.



Obrázek 15 OSPF. Zdroj: vlastní zpracování

V obrázku 15 jsou znázorněny celkem tři typy OSPF routerů:

- páteřní,
- hraniční,
- interní.

Směrovače jsou řazeny do kategorie podle členství v oblastech, do kterých spadají. Pojem interní nebo páteřní směrovač je celkem intuitivní a jeho význam lze vypozorovat dle jeho zařazení. Interní směrovač je takový, do kterého spadají všechna jeho rozhraní do stejné oblasti, kterou ovšem není „Oblast 0“. Interní routery si informace o směrovacích datech vyměňují napřímo mezi všemi routery ve své oblasti a také s jejich hraničními routery. Díky tomuto mechanismu je topologie v dané oblasti známa během krátké doby všem připojeným routerům a je zachována její stabilita. Hraniční směrovače jsou ty směrovače, které propojují interní a páteřní směrovače – jsou tedy na jejich rozhraní. I hraniční routery jsou

součásti výměny směrovacích informací. Hraniční routery ovšem spadají do více než jedné oblasti (oblasti 0 + oblast >0), proto musí zjišťovat informace ze všech hraničních oblastí. Výhodou je, že informace o topologii sítí zůstávají pouze v dotčených oblastech. Hraniční routery tyto informace slučují do souhrných dat, které si pak zase vyměňují mezi ostatními hraničními routery. Všechny routery v oblasti 0 jsou pak zásobeny informacemi o stavu a topologii v ostatních oblastech. Vzniká tak velice rychle přehled o topologii sítí. Páteřní směrovače tvoří základní skupinu routerů, přes které probíhá komunikace, pokud nedochází ke komunikaci pouze v jedné oblasti. Podle jejich pojmenování si můžeme vydefinovat jejich zásadní důležitost. Páteřní routery udržují informace nejen o jejich oblasti, ale o všech oblastech jejich autonomního systému. Ve spojitosti s těmito typy směrovačů lze určit dva typy směrování:

- uvnitř oblasti,
- mezi oblastmi.

Směrování uvnitř oblasti je uskutečněno dle obrázku 15 pouze mezi routery jedné oblasti směrovačem 5, 8 a 9. Pokud bude komunikace probíhat pouze mezi těmito routery, hovoříme pak o směrování uvnitř oblasti. Když se do komunikace zapojí i routery z jiných oblastí, pak se jedná o směrování mezi oblastmi. Pokud spolu budou komunikovat interní routery, musí být komunikace vedena přes oblast 0. Tímto řešením je zajištěno, aby nedocházelo ke složitým hierarchickým vazbám, ale strukturované hierarchické struktuře.

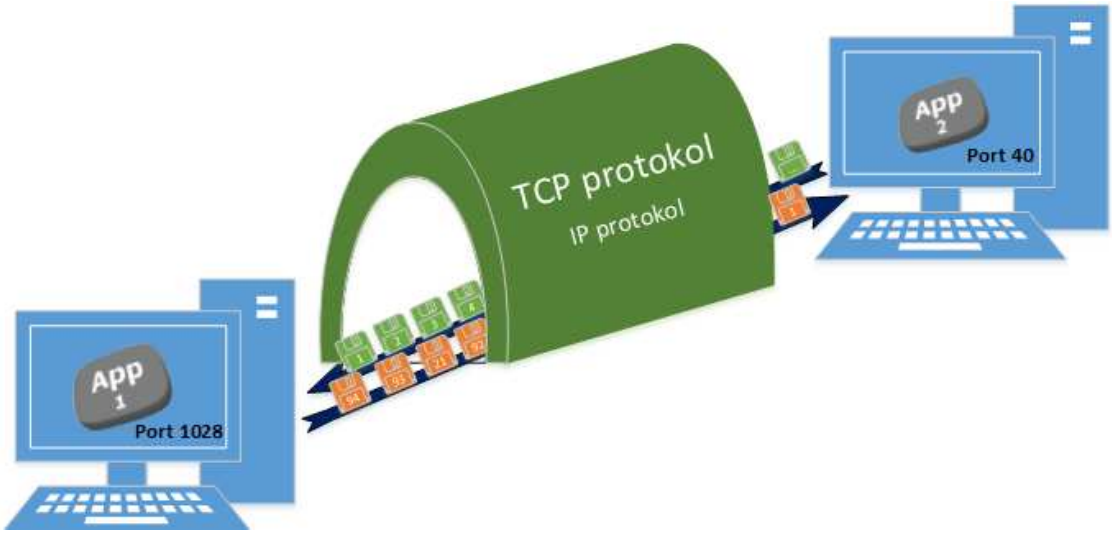
7.4 Transportní vrstva

Stejně jako u internetové (síťové) vrstvy se tato vrstva mnoho neliší jak v IOS/OSI modelu, tak v protokolu TCP/IP. Velmi jednoduše řečeno, na této vrstvě se žádné směrování neřeší, tuto službu přenechává službě nižších vrstev, jako kdyby pro ni žádná síťová infrastruktura neexistovala. Jejím úkolem je zajistit předání dat správné aplikaci na vzdáleném počítači.

7.4.1 Protokol TCP

TCP protokol je druhý z celého názvu protokolu TCP/IP. TCP protokol je protokolem vyšší vrstvy. Jaký je mezi nimi rozdíl?

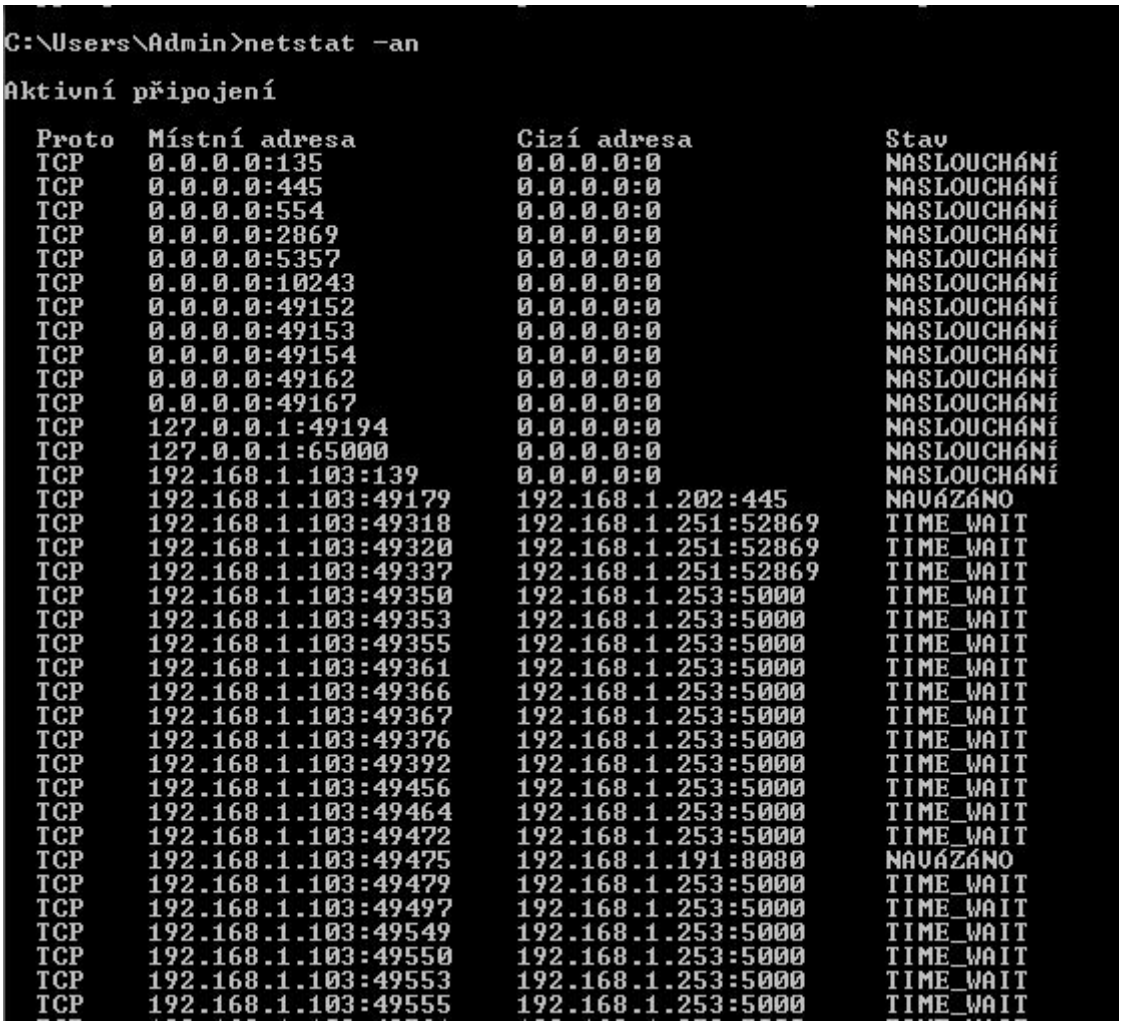
Zatím co protokol IP se zabývá směrováním v síti, tak TCP řeší pouze to, jak dostat přenášená data mezi spuštěnými aplikacemi. Z uvedeného vyplývá, že je zbytečné, aby dva protokoly řešily stejnou problematiku - TCP se routingem tedy již nezabývá. Naopak IP protokol se nevěnuje datům, která se ocitají na rozhraní pracovní stanice. Protokol TCP je služba, která je spojovaná. Spojový charakter jí umožňuje vytvářet takzvaný spojový tunel, kterým se data mohou současně přenášet oběma směry. Aby byla data přehledná, jsou data číslována. Pokud dojde ke ztrátě dat, nebo jejich poškození, vyžádá si příjemce nová náhradní data. K tomu, aby byla data směrována správně a ke správné aplikaci, nemůžeme v adresaci používat pouze IP adresu, ale musí být připojeno také číslo portu.



Obrázek 16 TCP tunel. Zdroj: vlastní zpracování

Číslo portu si můžeme v praxi představit jako velkou administrativní budovu, ve které sídlí více firem a vykonávají různé činnosti. Vzhledem k tomu, že se firmy nacházejí v určitých patrech budovy, lze je díky jejich poloze identifikovat. Např. firma, která má na starost údržbu, je v 1. patře. Pokud bychom chtěli této firmě předat balíček, museli bychom znát poštovní (IP) adresu budovy a vědět, že sídlí v prvním patře. První patro je tedy v případě doručování zásadní informace, stejně

tak jako u číslování portů aplikací. Bez směrování dat do aplikace by se data na určené místo nedostala.



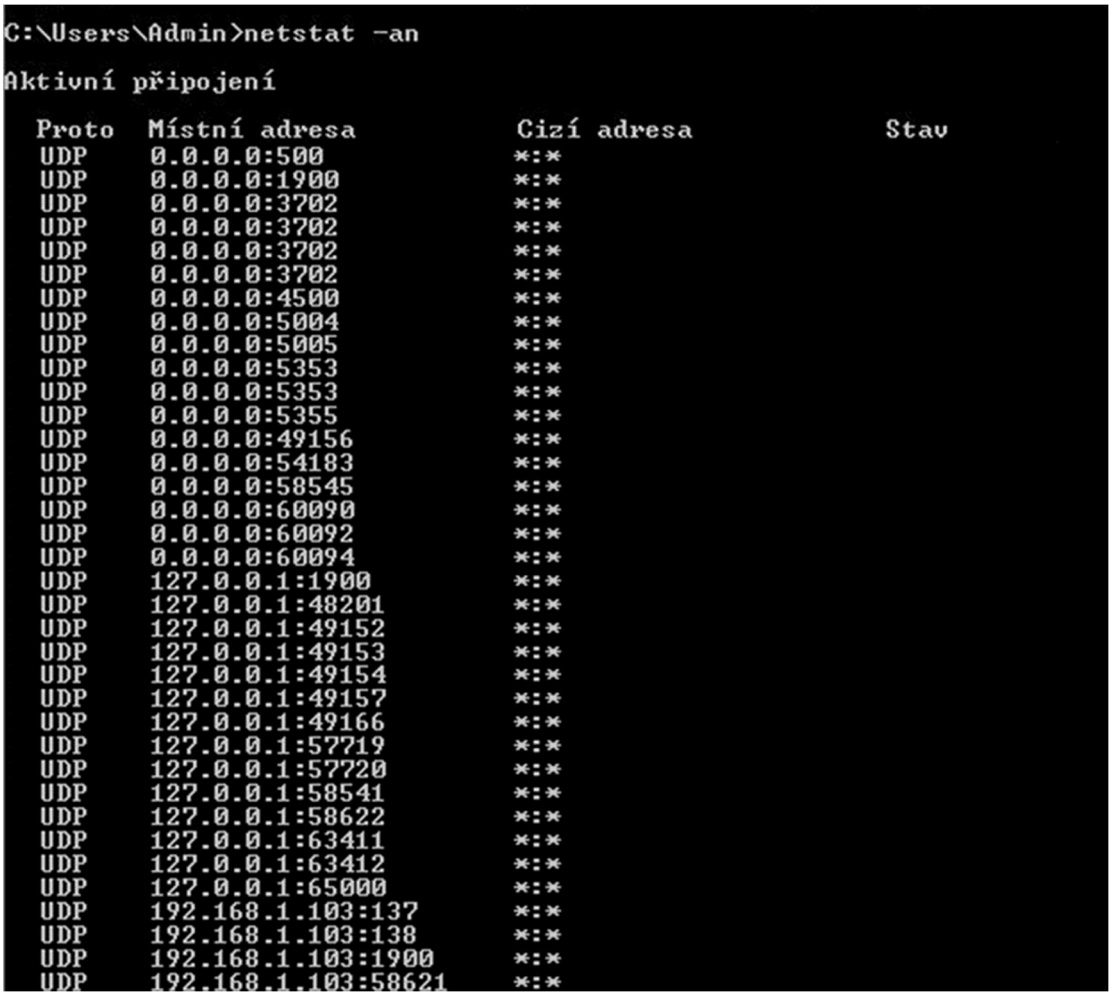
```
C:\Users\Admin>netstat -an

Aktivní připojení

  Proto  Místní adresa          Cizí adresa            Stav
  TCP    0.0.0.0:135            0.0.0.0:0              NASLOUCHÁNÍ
  TCP    0.0.0.0:445            0.0.0.0:0              NASLOUCHÁNÍ
  TCP    0.0.0.0:554            0.0.0.0:0              NASLOUCHÁNÍ
  TCP    0.0.0.0:2869           0.0.0.0:0              NASLOUCHÁNÍ
  TCP    0.0.0.0:5357           0.0.0.0:0              NASLOUCHÁNÍ
  TCP    0.0.0.0:10243          0.0.0.0:0              NASLOUCHÁNÍ
  TCP    0.0.0.0:49152          0.0.0.0:0              NASLOUCHÁNÍ
  TCP    0.0.0.0:49153          0.0.0.0:0              NASLOUCHÁNÍ
  TCP    0.0.0.0:49154          0.0.0.0:0              NASLOUCHÁNÍ
  TCP    0.0.0.0:49162          0.0.0.0:0              NASLOUCHÁNÍ
  TCP    0.0.0.0:49167          0.0.0.0:0              NASLOUCHÁNÍ
  TCP    127.0.0.1:49194        0.0.0.0:0              NASLOUCHÁNÍ
  TCP    127.0.0.1:65000        0.0.0.0:0              NASLOUCHÁNÍ
  TCP    192.168.1.103:139      0.0.0.0:0              NASLOUCHÁNÍ
  TCP    192.168.1.103:49179    192.168.1.202:445      NAVÁZÁNO
  TCP    192.168.1.103:49318    192.168.1.251:52869    TIME_WAIT
  TCP    192.168.1.103:49320    192.168.1.251:52869    TIME_WAIT
  TCP    192.168.1.103:49337    192.168.1.251:52869    TIME_WAIT
  TCP    192.168.1.103:49350    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49353    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49355    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49361    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49366    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49367    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49376    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49392    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49456    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49464    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49472    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49475    192.168.1.191:8080     NAVÁZÁNO
  TCP    192.168.1.103:49479    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49497    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49549    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49550    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49553    192.168.1.253:5000     TIME_WAIT
  TCP    192.168.1.103:49555    192.168.1.253:5000     TIME_WAIT
```

Obrázek 17 TCP relace - PC. Zdroj: Příkazový řádek MS Windows

Na počítači se můžeme podívat na výpis všech spojení protokolem TCP a UDP. Z toho obrázku je zřejmé, že jsou aplikacím vytvářeny spojové tunely. Každý řádek značí jedno spojení, které si udržuje určitý stav. Dále lze rozpoznat finální podobu odchozí (místní) adresy a cílové (cizí) adresy. IP adresa je již rozšířena o dvojtečku a číslo portu aplikace. Mimo jiné je zobrazen aktuální stav tohoto připojení.

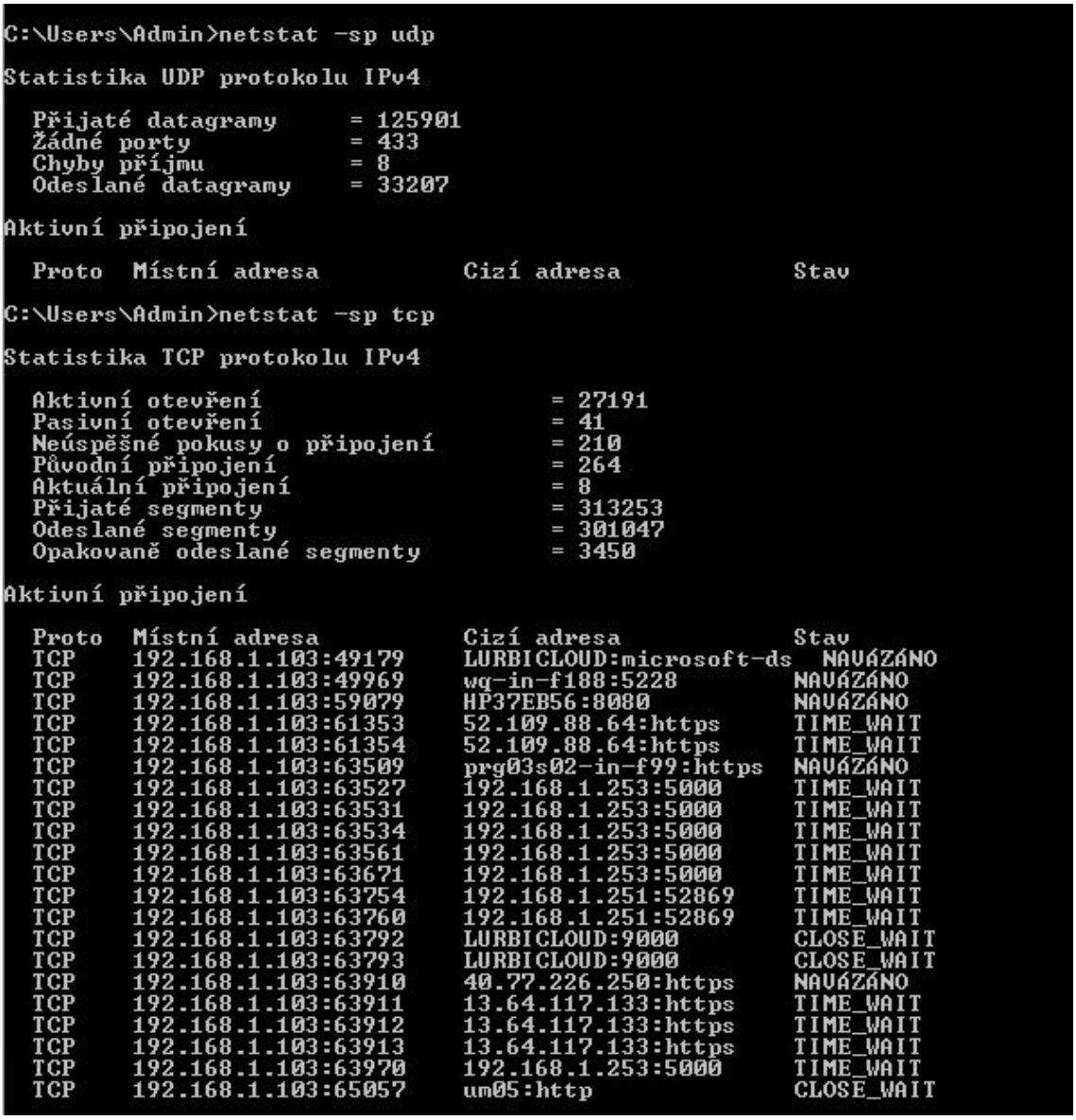
7.4.2 Protokol UDP

Protokol UDP je v mnoha ohledech podobný protokolu TCP. Lze jej definovat jako jednodušší alternativu protokolu TCP. Na rozdíl o protokolu TCP nevytváří spojový charakter, tzn., nezaobírá se podobou a celistvostí doručených datagramů. Kontrolní činnost nad daty je přenechána aplikační vrstvě. Porty jsou číslovány podobně jako u protokolu TCP. Je nutné upozornit na to, že ač může být číselné značení portů dost podobné jako u TCP, tak čísla portů u UDP nesouvisí s čísly portů u TCP.



Obrázek 18 UDP relace - PC. Zdroj: Příkazový řádek MS Windows

Na obrázku 19 je viditelný rozdíl mezi protokoly TCP a UDP - není udržován stav spojení, neboť UDP má nespojový charakter.



Obrázek 19 TCP/UDP rozdíl relací - PC. Zdroj: Příkazový řádek MS Windows

8 Praktická část práce – Směrování paketu od připojeného klienta k serveru GOOGLE DNS

8.1 Účel praktické části

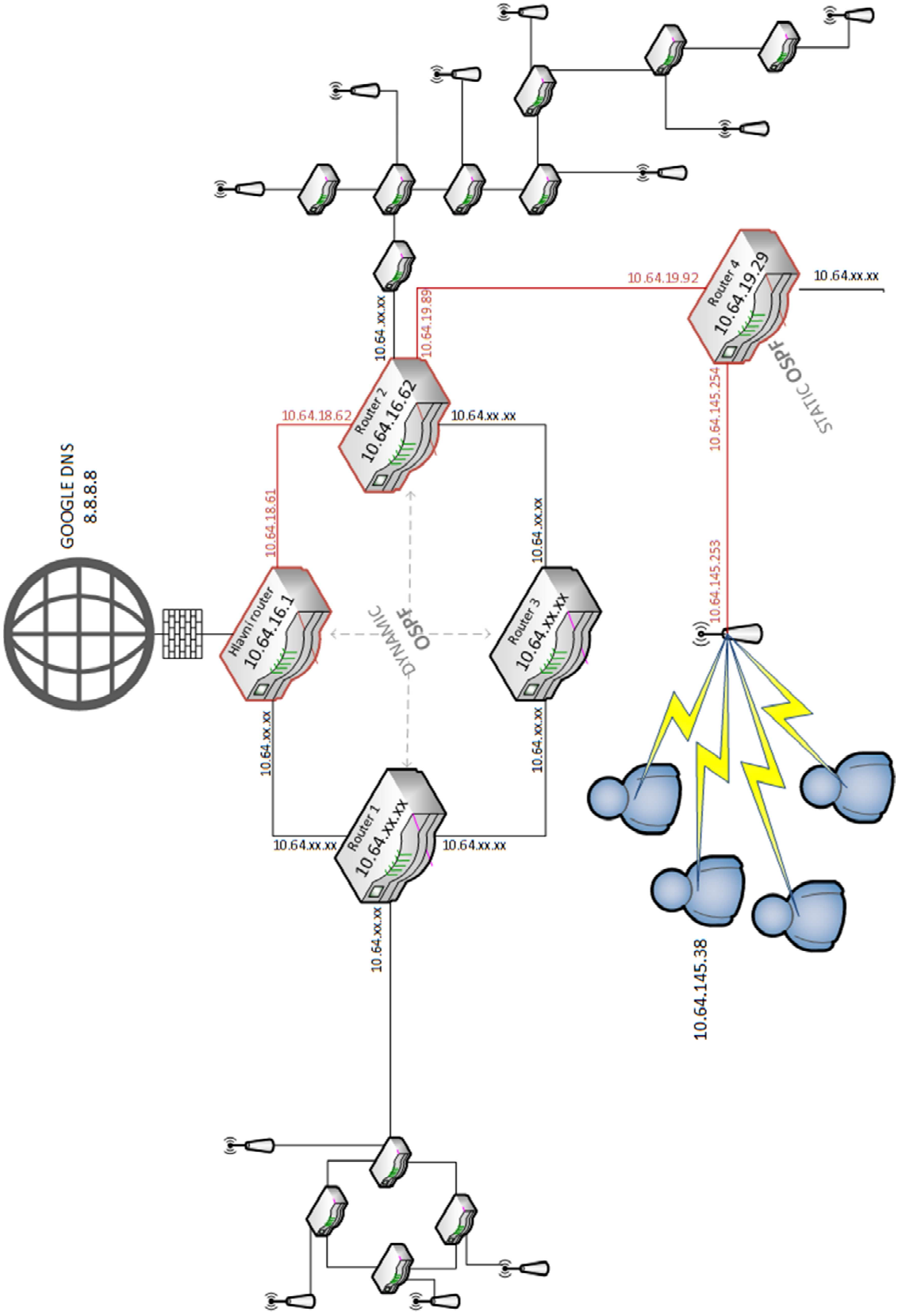
V praktické části práce budou aplikovány všechny dosavadní poznatky a budou ověřeny na praktické ukázce v reálné síti jednoho z poskytovatelů internetu. Bude vyslán požadavek od koncového zákazníka a podrobněji si zmapujeme, jak požadavek putuje síti. Ověříme naše doposud nasbírané informace přímo na tomto příkladu. Zanalyzujeme každý směrovač, přes který požadavek prošel, a ověříme, že naše informace o směrování jsou správné. Výsledkem této analýzy nebude samotné ověření principu směrování, ale i kontrola současného stavu a nastavení jednotlivých směrovačů, které v oblasti směrování hrají zásadní vliv. Proto bude praktická část rozdělena na dvě analyzační části:

- první část bude analyzovat a ověřovat správnost směrování požadavku sítí,
- druhá část ověří celkový stav znázorněné sítě, včetně jejího zabezpečení ve spojení se směrováním.

K tomu, aby vnitřní síť internetového providera byla stabilní a nebyla nevyvážená, je třeba ji hned v počátcích její tvorby správně navrhnout. Analyzovaný internetový poskytovatel působí na území o rozloze přes 120km^2 s celkovým počtem přes 1.000 aktivně připojených uživatelů. Tato síť je v současnosti tvořena 10-ti hlavními spoji v placeném licenčním pásmu, s 25-ti veřejnými přístupovými body a desítkami směrovacími routery. Pokud by byla síť směrována prostřednictvím pouze jedné komunikační větve, byla by v tento moment značně přetížena a v případě výpadku jakéhokoliv aktivního prvku by došlo k nefunkčnosti části sítě. Proto je při tvorbě topologie sítě vhodné vše řádně promyslet a vyhnout se tak do budoucna větším nepříjemnostem.

8.2 Analýza směrování požadavku

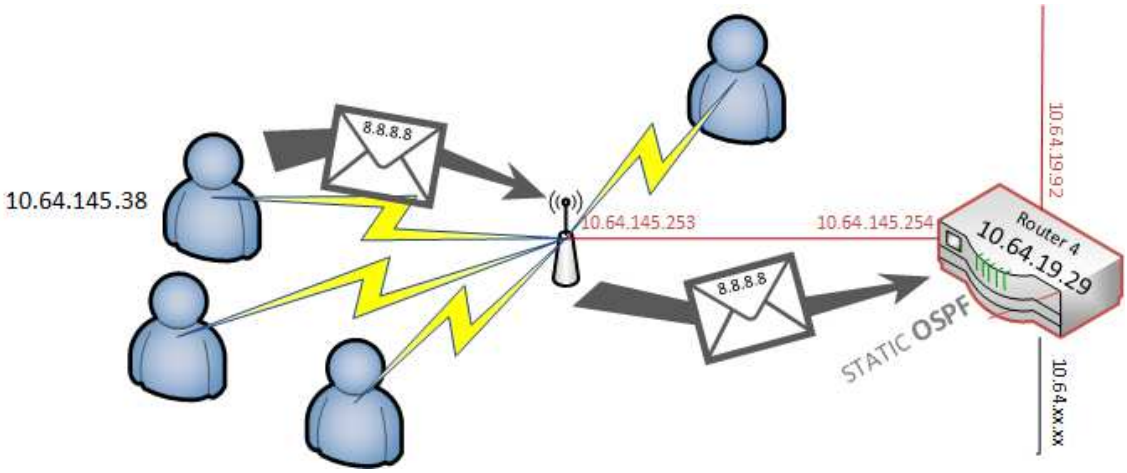
Analyzovanou část sítě znázorňuje obrázek 20. Jedná se o malou část sítě, na kterou je napojeno přibližně 50 uživatelů. Tato část je pouze jednou z mnoha dalších, kterými je síť tvořena. Uživatelé jsou k síti připojeni pomocí point-to-multipoint technologie. V praxi to znamená, že jsou uživatelé připojeni na jeden přístupový bod (CPE - Customer Premise Equipment), na který mají všichni přímou viditelnost a technologicky splňují požadavky pro připojení. Po připojení do sítě získá každý z uživatelů svojí vnitřní IP adresu z rozsahu IP adres přidělených v rámci přístupového bodu. Díky tvorbě podsítí může být síťovou bránou pro všechny připojené uživatele k jednomu přístupovému bodu právě tento přístupový bod. Díky tomuto známému bodu dochází k automatickému směrování v síti pomocí směrovače.



Obrázek 20 Provider – síť. Zdroj: vlastní zpracování

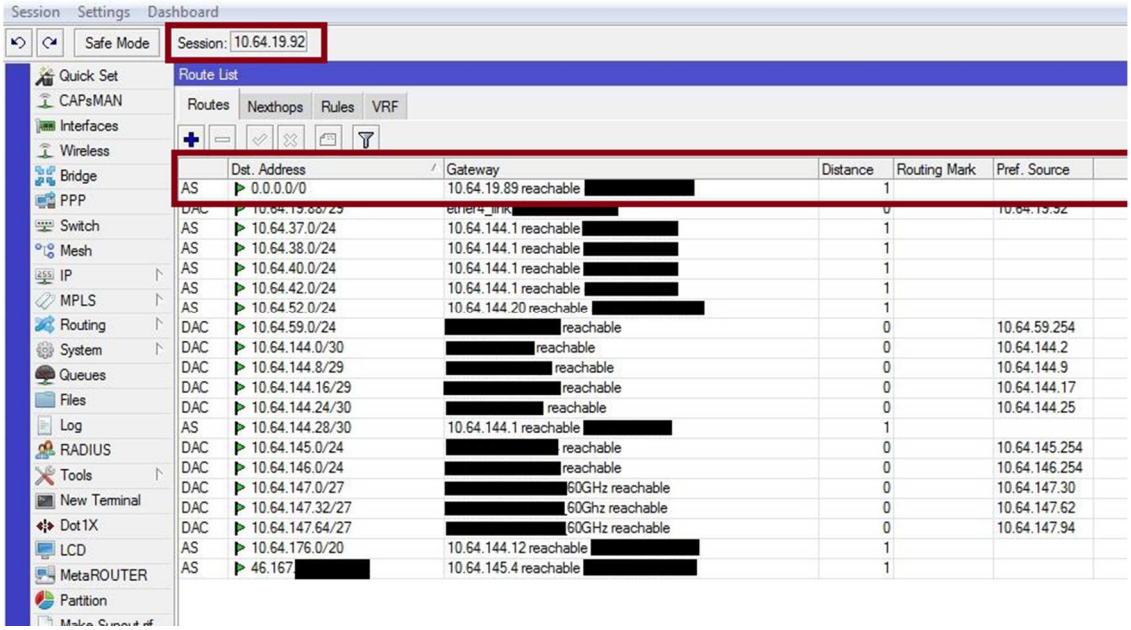
Názorně si zmapujeme z pohledu směrovačů případ, kdy uživatel s IP adresou 10.64.145.38 vyšle jakýkoliv požadavek na veřejný DNS server GOOGLE s veřejnou IP adresou 8.8.8.8.

Uživatel s vnitřní adresou 10.64.145.38 tedy vysílá požadavek, který je automaticky směrován na jeho bránu v síti 10.64.145.253, kterým je jeho přístupový bod. Přístupový bod má nastavenou svoji bránu 10.64.145.254, která je adresou prvního routeru v cestě - jedná se o router 4. Tato brána je již pevně definována v nastavení přístupového bodu. Tyto první předávky jsou detailněji znázorněny na obrázku 21.



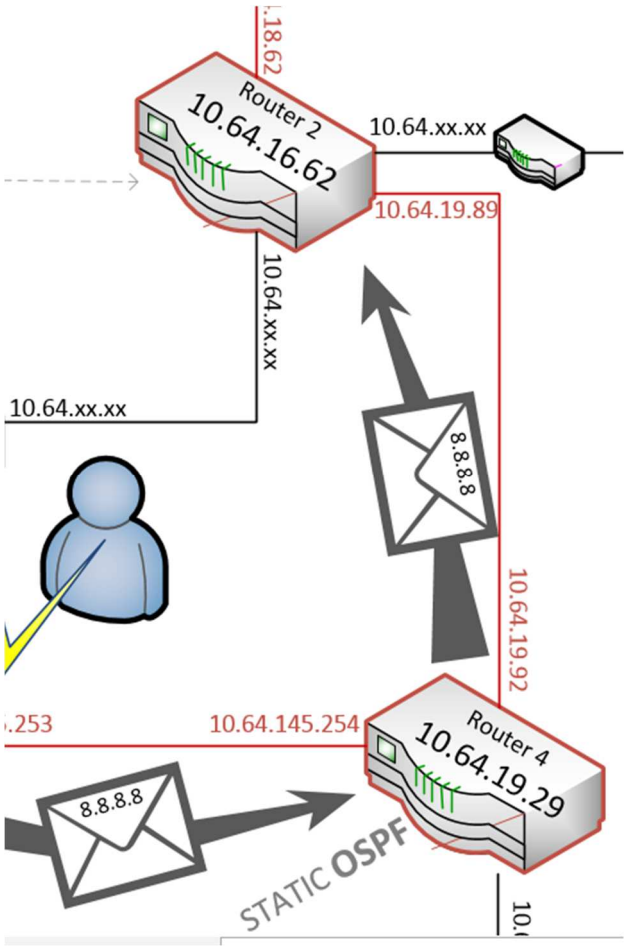
Obrázek 21 1. část sítě. Zdroj: vlastní zpracování

Do tohoto okamžiku nebylo pro zařízení problematické určit, jakým směrem bude požadavek směrovat. Nenastala situace, v které je nutné rozhodnout, jakou cestou budou data vyslána. Požadavek se aktuálně nachází na rozhraní routeru 4. Router 4 má směrovací protokol OSPF nastavený staticky. V praxi to znamená, že správce nastavil směrovací tabulku ručně. Ruční nastavení připadá v úvahu v případě, kdy se nejedná o velké množství spojení a je možné se v topologii okolí směrovače jednoduše orientovat.



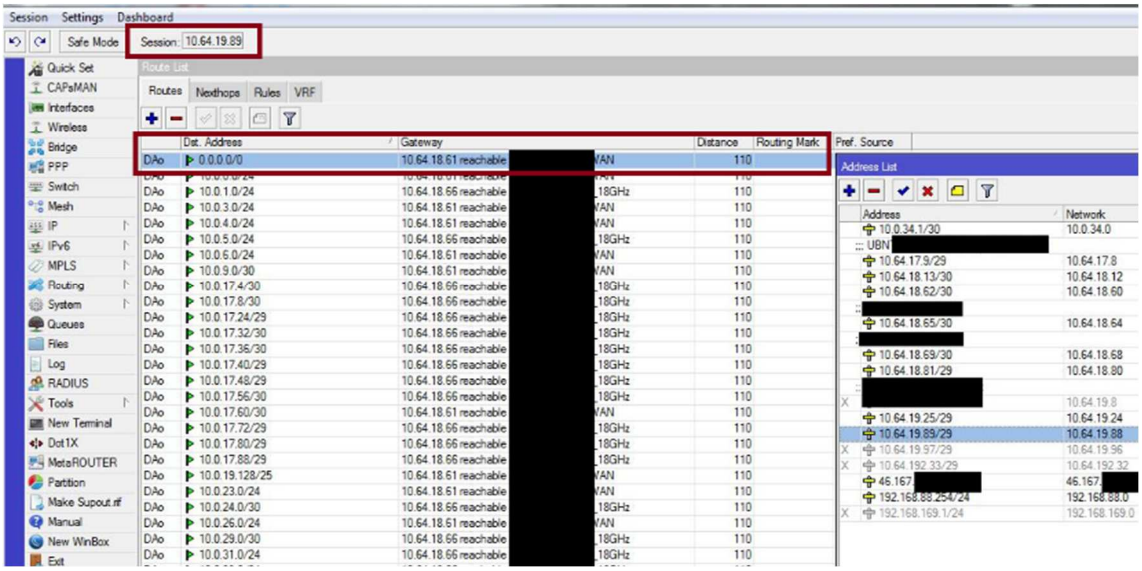
Obrázek 22 Routovací tabulka Winbox – router 4. Zdroj: vlastní zpracování

Na obrázku 22 je výpis směrovací tabulky routeru 4. Směrovací tabulka je pro přehlednost seřazena vzestupně, stejně tak v ní i samotný router vyhledává. V tomto případě je cílová adresa (8.8.8.8) směrována ven do sítě internetu, tomu přísluší hned první řádek ve směrovací tabulce s adresou 0.0.0.0 s cílovou bránou 10.64.19.89. Pro router to znamená, že veškerá data směrovaná na rozhraní routeru a dále do sítě, budou zasílána na rozhraní routeru 2. Ve směrovací tabulce se nachází větší počet záznamů, než je zobrazeno na obrázku 20. Důvodem je fakt, že obrázek nekoresponduje se skutečností. Struktura sítě je mnohem komplikovanější, což by znepřehlednilo obrázek. Skutečná je červeně vyznačená trasa, kterou budeme pro ukázku požadavku na DNS GOOGLU potřebovat.



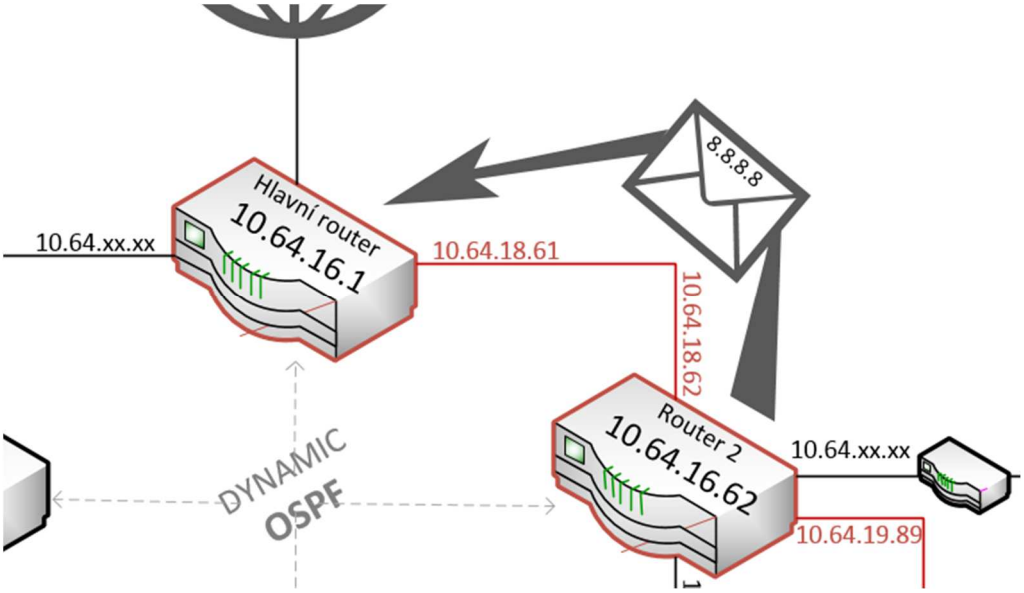
Obrázek 23 2. část sítě. Zdroj: vlastní zpracování

Prvním rozhodnutím byl požadavek vyslán na rozhraní routeru číslo 2 na IP adresu 10.64.19.89. Tento proces se odborně nazývá HOP (skok). V praxi pak jeden požadavek, než dorazí ke svému cíli, podstupuje od jednotek po desítky HOPů. Zatím se stále pohybujeme v prostředí vnitřní sítě poskytovatele, což je na první pohled rozpoznatelné dle IP adresy, na kterou dochází ke směrování.



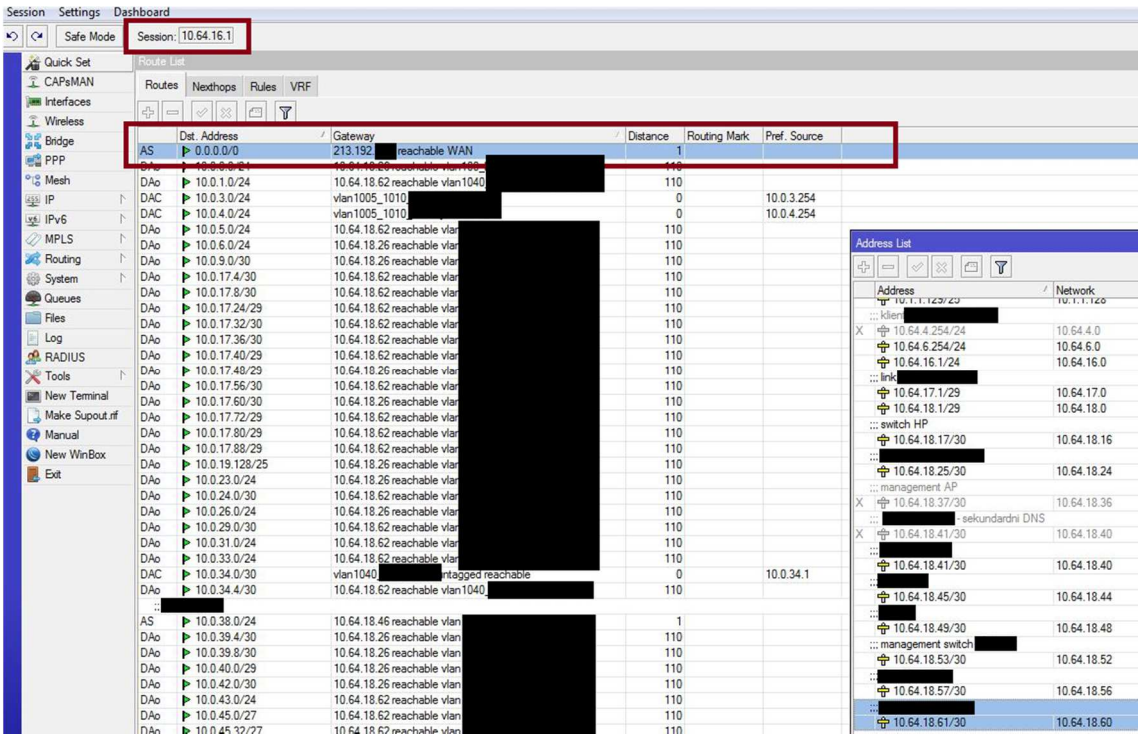
Obrázek 24 Routovací tabulka Winbox – router 2. Zdroj: vlastní zpracování

Router 4 z rozhraní 10.64.19.92 úspěšně přeposlal data na rozhraní routeru 2 s IP adresou 10.64.19.89. I zde se proces opakuje, pouze s tím rozdílem, že směrovací tabulka má jinou podobu - její počet směrovacích položek je několikrát větší než u routeru 4, který byl konfigurován staticky a neměl kolem sebe velký počet sousedících zařízení. Router 2 má od správce nastaveno dynamické směrování pomocí protokolu OSPF, který jsme si detailněji vysvětlovali. V rámci jedné záplavy se tedy router dozví vše potřebné o okolních připojených zařízení. Opět je směrovací tabulka seřazena vzestupně dle IP adres, proto není v tomto případě problém pro router určit cestu do internetu, která se nachází na prvním řádku. Adresa 0.0.0.0 se nachází za bránou 10.64.18.61.



Obrázek 25 3. část sítě. Zdroj: vlastní zpracování

Předáním dat na hlavní router došlo k poslední předávce v rámci vnitřní sítě poskytovatele, viz obrázek 25. Ze směrovací tabulky hlavního routeru si lze všimnout, že směr směrování tohoto požadavku již není interní, ale jedná se o veřejnou IP adresu směrovače primárního poskytovatele.



Obrázek 26 Routovací tabulka Winbox – hlavní router. Zdroj: vlastní zpracování

Ačkoliv se tento proces může zdát složitým, pro směrovače je toto banální a rutinní činnost. Pokud je vše správně navržené a nastavené, je zaslání požadavku z vnitřní sítě až na hraniční router s vnější sítí záležitostí pouze několika mili sekund.

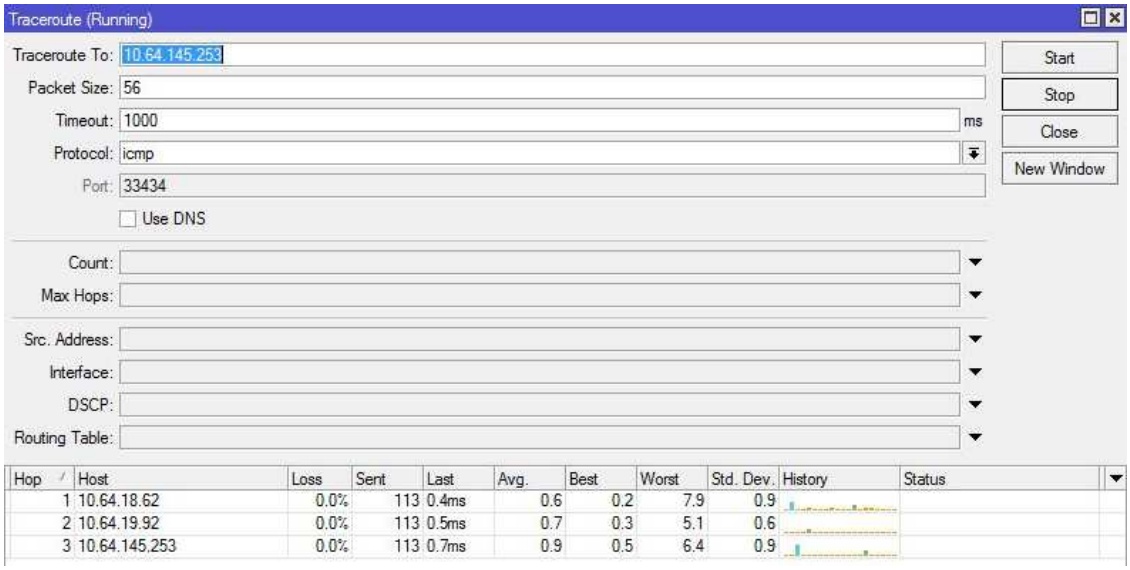
8.2.1 Ověření správnosti trasování

Správnost tohoto procesu můžeme jednoduše ověřit pomocí příkazu traceroute. Abychom nemuseli simulovat adresu uživatele, můžeme spustit trasování opačným směrem z hlavního routeru na adresu uživatele. Výsledek musí být totožný, pouze v opačném pořadí.

```
  MMM      MMM       KKK                          TTTTTTTTTTT      KKK
  MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.44.2 (c) 1999-2019       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level
[LUrbi@CER_router] > tool
bandwidth-server  mac-server  sigwatch  traffic-generator  dns-update  flood-ping  mac-telnet   profile    speed-test  wol
e-mail            netwatch    sms        traffic-monitor    export      ip-scan     memory-test  snmp-get   torch
graphing          romon       sniffer    bandwidth-test     fetch       mac-scan    ping-speed   snmp-walk  traceroute
[LUrbi@CER_router] > tool traceroute
count  dscp  duration  freeze-frame-interval  interface  max-hops  port  protocol  routing-table  size  src-address  timeout  use-dns  address
[LUrbi@CER_router] > tool traceroute address=10.64.145.253
 # ADDRESS                          LOSS SENT    LAST     AVG    BEST   WORST STD-DEV STATUS
 1 10.64.18.62                       0%    7   0.5ms     0.4     0.2     0.5     0.1
 2 10.64.19.92                       0%    7   0.5ms     0.7     0.4     1.8     0.5
 3 10.64.145.253                     0%    7   0.8ms     0.8     0.5     1.3     0.3
-- [Q quit|C-z pause]
```

Obrázek 27 MikroTik – TraceRoute. Zdroj: vlastní zpracování

Prvním routerem, na který se požadavek dostane, je hraniční router v našem pojmenování hlavní router s IP adresou 10.64.16.1. Hlavní router opět na základě směrovací tabulky rozhoduje, kam jsou data dále směrována. V našem případě se jedná o router 2 (10.64.18.62), který dále směruje k routeru 4 (10.64.19.92). Router 4 v posledním kroku směruje požadavek přímo na adresu cíle (10.64.145.253). Směrování tedy probíhá správně a dle popisu.

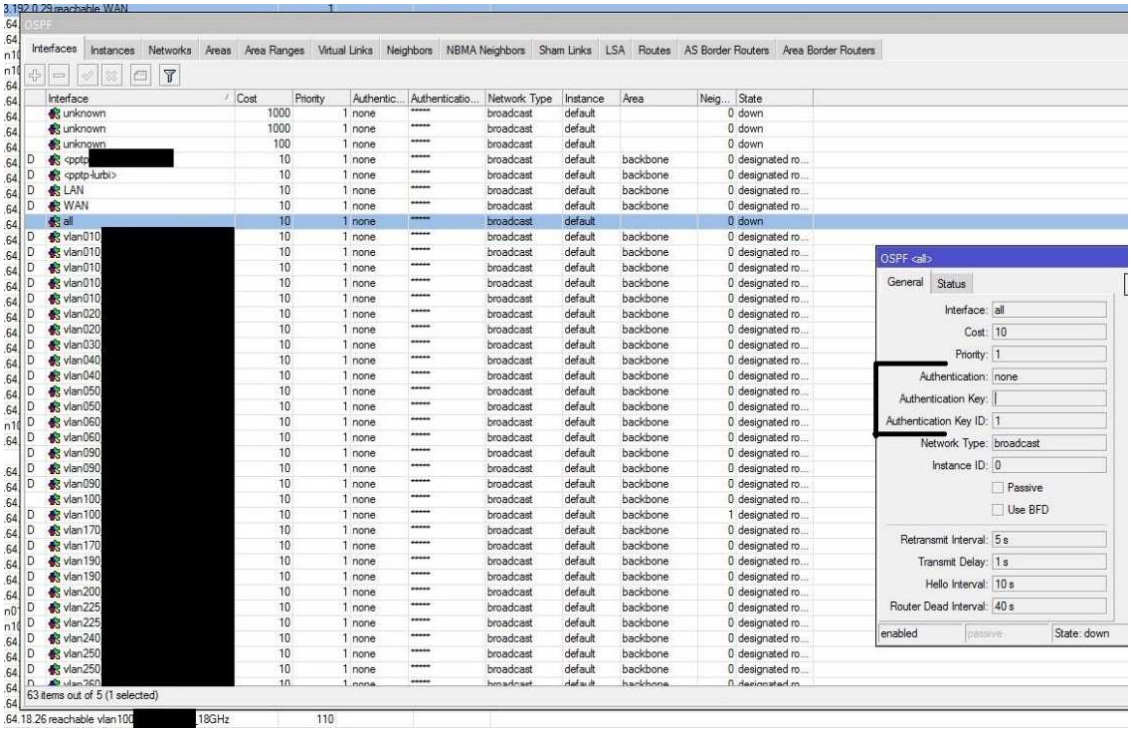


Obrázek 28 WinBox – TraceRoute. Zdroj: vlastní zpracování

8.3 Analýza celkového stavu

Základem sítě je si správně zvolit a nastavit celou topologii sítě, použití typů připojení a jejich správné konfigurace. U sledovaného poskytovatele bylo na vše potřebné myšleno, proto není třeba navrhovat žádné změny a úpravy v topologii a typu zařízení.

Při analýze vnitřní topologie a nastavení aktivních prvků je dobré se zaměřit i na oblast zabezpečení směrování v síti, která na žebříčku důležitosti určitě patří do jedné z nejdůležitějších skupin. Celkově je síť velice dobře a promyšleně navržená a zabezpečená. Ovšem při analýze nastavení OSPF byl objeven bezpečností nedostatek, který by umožňoval zdatnému uživateli z vnitřní sítě škodit. V nastavení OSPF bylo historicky nastaveno rozhraní „all“, které nebylo nijak zabezpečeno, viz obrázek 29. V tomto momentu by bylo možné přesměrovat komunikaci. V důsledku by mohlo dojít k narušení veškeré komunikace, která byla vysílána. Tato situace by pro poskytovatele znamenala komplikace při poskytování služby, proto v rámci analýzy došlo k okamžité nápravě tohoto bezpečnostního nedostatku. V praxi by to pak znamenalo, že by záplava byla směrována broadcastovou zprávou na všechna rozhraní hlavního routeru.



Obrázek 29 WinBox – OSPF all. Zdroj: vlastní zpracování

8.3.1 Návrh na zlepšení zabezpečení nastavení OSPF v hlavním routeru

Při analýze celkového stavu nastavení sledované části sítě byl objeven nedostatek v zabezpečení OSPF zpráv. Broudcastová zpráva zasílaná na všechna zařízení v této síti s sebou nenesla žádný typ zabezpečení. Pro zasvěceného uživatele, který by se v této síti nacházel, by nebyl žádný problém tuto zprávu zachytit a změnit její výsledný obsah, ve kterém by mohl nastavit směrování na jiné zařízení (například sebe). Následně by se na jeho adresu dostávala cizí data, která by mohl znovu odposlouchávat.

Zmiňovaný poskytovatel byl na tento nedostatek neprodleně upozorněn. Následně došlo ze strany poskytovatele k okamžité nápravě, kdy byla provedena změna v nastavení OSPF.

9 Shrnutí výsledků

Bakalářská práce se zabývala obecným popisem problematiky, kterou bylo směrování v síti na základní úrovni. Měla za cíl nastínit, jak ke směrování dochází a co za ním stojí. Vzhledem k samotné složitosti a obšírnosti, v které se toto téma nacházelo, byly v bakalářské práci popsány primárně služby a pojmy nutné k pochopení praktické části. Je simulován postup požadavku. Požadavek procházel od koncového uživatele směrem do internetu. V praktické části se převedly všechny tyto poznatky do praxe. Práce poukazuje na složitost, kterou s sebou obor nese a má za úkol nastínit, jak k samotnému směrování dochází. Ač principy směrování procházejí vývojem, základní myšlenka je postavena na základním modelu – ISO/OSI. Proto bylo nejprve nutné pochopit logiku rozdělení do základních síťových vrstev. V dalších krocích je jednoduší pochopit jeden z nejpoužívanějších směrovacích protokolů TCP/IP. Pro naše potřeby je zásadní pochopit první tři vrstvy, které jsou základem směrování. Proto byl v této práci kladen největší důraz právě těmto třem vrstvám. Důležitým tématem ve směrování byly směrovací tabulky, na základě kterých se routery rozhodují, kam data budou směrovat. O tom, jak se tyto směrovací tabulky plní, z velké části rozhodují správci sítě. V analyzované síti se v plné míře používá protokol OSPF, proto je pozornost věnována právě tomuto protokolu.

Během analýzy bylo detekováno slabé místo v nastavení zabezpečení. Díky doporučení došlo k zabezpečení pomocí hesla. K rozšíření obzorů v této tématice bych doporučil literaturu, ze které jsem čerpal a která se směrováním zabývá.

10 Seznam použité literatury

[1] ČESKO. § 42 zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 18. 3. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2013-304#p42

[2] ČESKO. § 97 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 18. 3. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-127#p97-3

[3] ČESKO. § 2 odst. 3 písm. a) vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 18. 3. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-357#p2-3-a

[4] ČESKO. § 73 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 18. 3. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-127#p73

[5] BIGELOW, Stephen J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Brno: Computer Press, 2004. ISBN 80-251-0178-9.

[6] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 978-80-251

[7] Přispěvatelé Wikipedie, Ethernet [online], Wikipedie: Otevřená encyklopedie, c2020, Datum poslední revize 8. 03. 2020, 12:44 UTC, [citováno 18. 03. 2020] https://cs.wikipedia.org/w/index.php?title=Ethernet&oldid=18238440

[8] BŘEHOVSKÝ, Petr. Praktický úvod do TCP/IP. Druhé vydání. České Budějovice: Kopp, 1995. ISBN 80-85828-29-4.

[9] KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

[10] SHINDER, Debra Littlejohn. Počítačové sítě: nepostradatelná příručka k pochopení sítové teorie, implementace a vnitřních funkcí [sic]. Praha: SoftPress, c2003. Cisco systems. ISBN 80-86497-55-0.

[11] ODOM, Wendell. Počítačové sítě bez předchozích znalostí. Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0538-5.

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

[13] 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.

11 Přílohy

1) oskenované zadání práce

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2019/2020

Studijní program: Systémové inženýrství a informatika
Forma: Kombinovaná
Obor/komb.: Informační management (im3-k)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Urban Lukáš	Malá 135, Hradec Králové - Pouchov	I1700276

TÉMA ČESKY:

Analýza a optimalizace routingu a zabezpečení v prostředí lokálního internetového providera

TÉMA ANGLICKY:

Analysis and optimization of routing and security in the environment of a local Internet provider

VEDOUCÍ PRÁCE:

Mgr. Josef Horálek, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce bude provést analýzu stávajícího stavu sítě lokálního providera a návrh optimalizace internetové konektivity s důrazem na routing a zabezpečení. V teoretické části práce autor představí principy a povinnosti lokálního providera a postup pro analýzu. V praktické části autor představí výsledky provedené analýzy a navrhne optimalizaci provozu a jeho zabezpečení včetně analýzy dopadů (BIA).

SEZNAM DOPORUČENÉ LITERATURY:

LAMMLE, Todd. CCNA routing and switching complete study guide. Second edition. United States?: Sybex, a Wiley brand, [2016]. ISBN 9781119288282.
GERARDUS, Blokdyk. Internet Provider Security a Complete Guide. 2018. 1: 5starcooks. ISBN 9780655316985.

Podpis studenta: ..... Datum: 13.2.2019

Podpis vedoucího práce: ..... Datum: 13.2.2019