
Evropský sociální fond
Praha & EU: Investujeme do vaší budoucnosti

# Základy adresace v počítačových sítích

**Ondřej Votava**
votavon1@fel.cvut.cz

# 1 Úvod

Tento materiál se zaměřuje pouze na protokolovou rodinu TCP/IP, konkrétně ve verzi 4. I přes nedostatek IPv4 adres je tento protokol stále nejpoužívanější a jeho použití v malých sítích je velice jednoduché. Po přečtení tohoto materiálu byste měli znát pojmy adresa, síť, podsíť, nadsíť, maska, třídní a beztřídní adresa a vědět, jak se mohou využít v počítačových komunikacích.

# 2 Základní pojmy

## 2.1 IP adresa

IPv4 adresa je 32 bitů dlouhé číslo [1]. Pro snažší manipulaci s tímto číslem je rozděleno na osmice bitů oddělené tečkami. Na obrázku 1 je znázorněna adresa v binárním tvaru a její přepis do běžného formátu v dekadickém zápisu.

| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 192 | | | | | | | | 168 | | | | | | | | 1 | | | | | | | | 135 | | | | | | | | |

192.168.1.135

*Obrázek 1: IPv4 adresa v binárním a dekadickém zápisu.*

| | **Zdroj** | **Cíl** |
|---|---|---|
| **IP adresa** | 10.0.2.56 | 10.0.1.30 |
| **Maska** | 22 (255.255.252.0) | neznámá |

1. Výpočet adresy sítě zdrojové stanice

| | | | | |
|---|---|---|---|---|
| **Adresa zdroje** | 00001010 | 00000000 | 00000010 | 00111000 |
| **Maska zdroje** | 11111111 | 11111111 | 11111100 | 00000000 |
| **Adresa sítě zdroje** | 00001010 | 00000000 | 00000000 | 00000000 |

2. Ověření, zda cíl je ve stejné síti, jako zdroj (první pravidlo směrovací tabulky 6)

| | | | | |
|---|---|---|---|---|
| **Adresa cíle** | 00001010 | 00000000 | 00000001 | 00011110 |
| **Maska zdroje** | 11111111 | 11111111 | 11111100 | 00000000 |
| **„Adresa sítě“ cíle** | 00001010 | 00000000 | 00000000 | 00000000 |

*Obrázek 2: Výpočet adresy sítě za použití masky.*

Adresa slouží k identifikaci *rozhraní* počítače. Má-li počítač více síťových karet, musí mít každá karta vlastní adresu. IP adresy se nacházejí na 3. vrstvě modelu ISO/OSI a jejich primárním cílem je zavést hierarchickou strukturu sítě.

## 2.2 MAC adresa

MAC adresy (Medium Access Control, řízení přístupu k médiu) jsou používány na 2. vrstvě modelu ISO/OSI. V sítích založených na technologii Ethernet má MAC adresa délku 48 bitů [2]. Pro snadnější práci s adresami jsou rozděleny do šesti skupin dvou hexadecimálních číslic, které bývají odděleny buď dvojtečkou nebo pomlčkou, např. 00:60:b3:6a:69:b0 nebo 00-60-b3-6a-69-c1. Výrobce síťových karet má vždy přidělen nějaký prefix, kterým adresy jeho karet vždy začínají, a zbytek adresy je přidělen výrobcem jednoznačně. MAC adresy jsou tedy unikátní[1] a z principu je jich přidělování nad nimi nelze vybudovat hierarchii.

## 2.3 Adresa sítě, maska sítě

IP adresy nemají žádnou vazbu na MAC adresy a proto je možné vytvářet hierarchii IP adres pouze jejich vhodným přidělováním. Pojem *adresa sítě* se opírá o lokální síť, kdy je vhodné, aby všechny stanice umístěné v jedné fyzické síti byly součástí jedné IP sítě. Pro vnější svět lze pak všechny stanice v této lokální síti identifikovat dvojicí hodnot, adresou sítě a její maskou.

*Maska sítě* je číslo, které udává, jak velká je daná síť. Lze ji zapsat buď jako obyčejné číslo z rozsahu 0 až 32 nebo jako IP adresu, která má specifické hodnoty. Číselná reprezentace udává, kolik bitů zleva má hodnotu 1, např. pro masku 8 to bude `11111111` a zbytek samé nuly, v zápisu formou IP adresy má maska 8 podobu 255.0.0.0. Jak velká síť bude, lze vypočítat velice jednoduše. Maska určuje, které bity se nesmějí měnit pro danou síť, ty jsou označeny jedničkami, bity, které nesou hodnotu 0, je možné v rámci sítě měnit. Pokud má tedy maska hodnotu 24, tedy maska obsahuje 24 jedniček, pak z IP adresy zbylo pouhých 8 bitů, které lze měnit. Počet adres v dané síti je tedy $2^{32-24} = 2^8 = 256$. Platí pravidlo, že nejnižší adresa dané sítě, tedy ta, kde jsou samé nuly, je považována za adresu sítě a nesmí být přidělena žádné stanici, naopak nejvyšší adresa sítě, tedy ta, kde jsou samé jedničky, je rezervována pro *broadcast*, tedy vysílání zpráv všem stanicím v dané síti. Proto je počet stanic, které lze umístit v síti vždy od dvě menší, např. pro masku 24 je to 254 stanic, pro masku 30 jsou to pouhé 2 stanice.

Maska je velice důležitá jak pro směrování , kdy nám umožňuje slučovat sítě do jednoho záznamu [3], tak pro komunikaci v rámci lokální sítě. Dvě stanice v lokální síti mohou komunikovat přímo, neboť mají přístup ke stejnému médiu, stanice, které jsou v různých fyzických sítích, musí využít prostředníka, který je připojen k oběma sítím. Při rozhodování, zda využít prostředníka, se stanice opírá o své směrovací tabulky[2], v nich jsou uloženy informace o masce sítě.

Ukažme si nyní jednoduchý příklad, kdy stanice zjistila, že její síťová adresa je 10.0.2.56/22 a chce poslat zprávu stanici s adresou 10.0.0.30. Ze své směrovací tabulky ví, že přímo připojená síť má

1 Nutný požadavek je, aby MAC adresa byla unikátní v každém síťovém segmentu (lokální síti).
2 Detailněji se jimi zabývá kapitola 3.3Směrování zpráv.

masku 22. S touto znalostí pak provede několik operací, aby zjistila, zda je cílová stanice v přímo připojené síti.

1. $my_network = $my_ip AND $mask {provede operaci logický součin vlastní IP adresy s maskou, viz. obrázek 2, první krok}
2. $target_network = $target_ip AND $mask {provede operaci logický součin IP adresy cíle s maskou, viz. obrázek 2, druhý krok}
3. **if** ($my_network == $target_network ) SEND_DIRECT {více v kapitole 3.1Komunikace na stejné síti}
4. **else** SEND_USING_GATEWAY {více v kapitole 3.2Komunikace mezi sítěmi}

## 2.4 Třídy adres

V počátcích byly definovány tři základní třídy adres [1], každá třída obsahovala balík adres a podle velikosti organizace, která požadovala adresy, byla vždy přidělena jedna síť z odpovídající třídy. Základní dělení tříd a jejich vlastnosti shrnuje tabulka 1.

V třídním systému adres hrál důležitou roli první byte adresy. Podle něho se dá usoudit, z jaké třídy je daná adresa a tudíž i jakou masku má daná síť. To zjednodušovalo práci se směrovacími záznamy. Třídní adresy, tak jak byly navrženy, však plýtvaly adresami, proto byl představen beztřídní způsob adresace, viz. kapitola 2.6.

| Třída | Základní vlastnosti |
|---|---|
| **A** | 0xxxxxxx \| \| \| <br> Maska 8, 24 bitů pro stanice, adresy z rozsahu 0 – 127.x.y.z |
| **B** | 10xxxxxx \| \| \| <br> Maska 16, 16 bitů pro stanice, adresy z rozsahu 128 – 191.x.y.z |
| **C** | 110xxxxx \| \| \| <br> Maska 24, 8 bitů pro stanice, adresy z rozsahu 192 – 223.x.y.z |

*Tabulka 1: Třídy adres A,B a C.*

## 2.5 Podsíť, nadsíť

Jak jsme již zmínili, je vhodné, aby pro jednu fyzickou síť existovala jedna IP síť. Jestliže však organizace získala síť ze třídy A, pak by její síť musela být ohromná, $2^{24}$ stanic je velice těžké udržovat a při použití sítě ethernet, kdy by všechny stanice sdílely jediné médium, by nebyla propustnost sítě nejvyšší. Proto vznikly tendence sítě rozdělit na menší celky, *podsítě* [4,5]. V tabulce 2 je zobrazena síť 192.168.10.0/24, která je rozdělena do 4 podsítí s maskou 26. Opačně se lze dívat na 4 sítě s maskou 26 jako na jednu nadsíť, která spojuje všechny tyto sítě do jedné nadsítě s maskou 24.

Všimněte si, že v tabulce 2 je adresa Podsítě 1 je identická s adresou Sítě. Tento překryv mohl být problematický, proto se Podsíť 1 dlouho nesměla používat [4]. Obdobným problémem trpí i Podsíť 4. Její nejvyšší adresa je totožná s adresou broadcastu celé Sítě, proto i tato adresa nesměla být využita. Tato omezení byla zrušena v novějším RFC 1860 [5], které definuje všechny možné podsítě. Podle [5] lze v tomto případě využít všechny 4 podsítě.

| **Síť** | 11000000 | 10101000 | 00001010 | 00000000 |
|---|---|---|---|---|
| **Maska sítě** | 11111111 | 11111111 | 11111111 | 00000000 |
| **Maska podsítě** | 11111111 | 11111111 | 11111111 | 11000000 |
| **Podsíť 0** | 11000000 | 10101000 | 00001010 | 00000000 |
| **Podsíť 1** | 11000000 | 10101000 | 00001010 | 01000000 |
| **Podsíť 2** | 11000000 | 10101000 | 00001010 | 10000000 |
| **Podsíť 3** | 11000000 | 10101000 | 00001010 | 11000000 |

*Tabulka 2: Síť, podsíť a nadsíť, modře je vyznačen prostor pro stanice.*

## 2.6 Beztřídní adresy

S přibývajícím počtem uživatelů Internetu začaly rychle ubývat volné adresy. Ukázalo se, že ne všichni vyžadují tak velké sítě, jako byly ve třídách A a B. Velké množství sítí nedokázalo využít celý adresní prostor, naopak spoustě sítím tento prostor chyběl, protože nevyužité adresy byly součástí již obsazených sítí. V RFC 1519 [3] byly zrušeny všechny třídní adresy a byla navržena opatření, která umožní agregaci směrovacích záznamů (vytváření nadsítí) a efektivnější přidělování adres. Nyní je nutné při použití adresy sítě vždy uvést i masku sítě.

## 2.7 Privátní sítě

Protokoly Internetu (IP) začaly být velice oblíbené a byly nasazovány i do sítí, které nebyly nebo neměly být připojeny k Internetu. Pro tyto sítě byly vyhrazeny 3 bloky adres, které se nesmí vyskytovat na Internetu a je povinností každého směrovače, který dostane zprávu pro/od takové adresy, aby tuto zprávu zahodil nebo provedl překlad adres. Tyto adresy jsou zachyceny v tabulce 3.

| **Síť** | **Počáteční adresa** | **Koncová adresa** |
|---|---|---|
| 10.0.0.0/8 | 10.0.0.0 | 10.255.255.255 |
| 172.16.0.0/12 | 172.16.0.0 | 172.31.255.255 |
| 192.168.0.0/16 | 192.168.0.0 | 192.168.255.255 |

*Tabulka 3: Adresy privátních sítí.*

## 2.8 Speciální adresy

Některé adresy nabývají specifického významu, jak už jsme si ukázali, adresa se samými nulami je adresa sítě, adresa se samými jedničkami je adresa broadcastu. Některé další specifické adresy shrnuje tabulka 4.

| Síť | Význam |
|---|---|
| 0..0 | Tento počítač na této síti |
| Síť.0..0 | Adresa sítě |
| Síť.Subsíť.0..0 | Adresa podsítě |
| Síť.1..1 | Brodcast do sítě (i všech podsítí) |
| Síť.Subsíť.1..1 | Broadcast do podsítě |
| 1..1 | Broadcast na lokální síti |
| 127.0.0.0/8 | Loopback |
| 169.254.0.0/16 | Link Local (RFC 3330) |

*Tabulka 4: Speciální adresy.*

# 3 Spolupráce 2. a 3. vrstvy při směrování

Když chce stanice A poslat zprávu stanici B, musí provést sérii kroků.

1. Vytvořit packet, v němž bude vyplněna adresa cíle (IP B) a odesilatele (IP A).
2. Najít vhodný záznam ve směrovací tabulce.
3. Umístit packet do rámce protokolu 2. vrstvy a správně vyplnit adresu cíle a odesilatele (např. MAC adresa A). Hodnota pro adresu cíle se bude lišit v závisloti na výsledku předchozího kroku.
4. Odeslat zprávu.

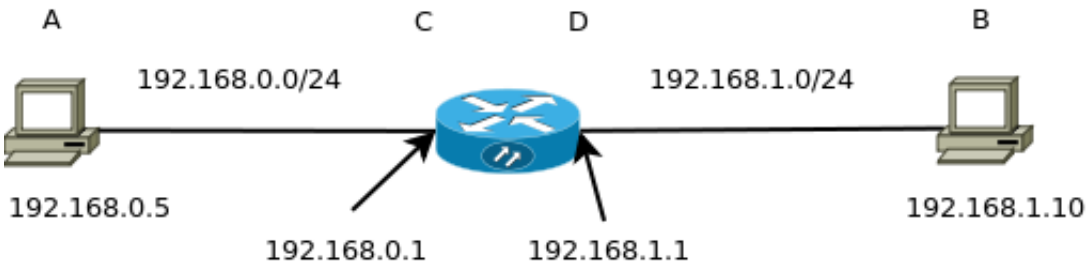
Postup, který je zahrnut v bodě 2 a 3 si nyní důkladně vysvětlíme.

| ff:ff:ff:ff:ff:ff | MAC A | Who has IP B? Tell IP A. | CRC |
|---|---|---|---|

*Obrázek 3: Zjednodušená struktura ARP dotazu.*

| MAC A | MAC B | B is 00:60:b3:6a:69:64 | CRC |
|---|---|---|---|

*Obrázek 4: Zjednodušená struktura ARP odpovědi.*




*Obrázek 5: Topologie jednoduché sítě.*

## 3.1 Komunikace na stejné síti

Jak již bylo naznačeno v kapitole 2.3, směrovací tabulka stanice obsahuje informace, jak vhodně zacházet s různými packety. Každá taková informace je zapsána na samostatném řádku a obsahuje několik hodnot, viz. kapitola 3.3. V tuto chvíli nás pouze zajímá, že ve sloupci Gateway je pro přímo připojené sítě uložena hodnota 0.0.0.0. Pokud tedy stanice v kroku 2 našla řádek, kde je Gateway nastavena na 0.0.0.0, pak se do políčka cílová adresa na 2. vrstvě napíše přímo adresa stanice B, např. MAC B. Zpráva pak bude mít formát, který je zachycen na obrázku 6.

| MAC B | MAC A | IP B | IP A | Zpráva | CRC |
|---|---|---|---|---|---|

*Obrázek 6: Zjednodušený formát zprávy od A k B.*

Častým problémem však může být, že stanice A zná pouze IP adresu stanice B. Tato situace nastává vždy po startu počítače, kdy stanice „nějak zjistí[3],“ jakou IP adresu má např. DNS server. Když tedy bude chtít A komunikovat s tímto serverem, zná jen jeho IP, nikoliv MAC. Aby byla stanice A schopna zjistit, jakou MAC adresu má DNS server, využije protokol ARP [6].

### 3.1.1 ARP

Address Resolution Protocol [6] umožňuje zjistit, jakou MAC adresu má rozhraní s konkrétní IP adresou. Při tom využívá toho, že podobně, jako je v IP adresa se samými jedničkami reprezentována jako broadcast, úplně stejně je MAC adresa se samými jedničkami reprezentována jako broadcast, tedy zprávu zaslanou na adresu ff:ff:ff:ff:ff:ff přijmou všechny stanice a postoupí ji ke zpraco-

| MAC **C** | MAC A | IP B | IP A | Zpráva | CRC |
|---|---|---|---|---|---|

*Obrázek 7: Zjednodušená struktura zprávy od A.*

| MAC G | MAC H | IP B | IP A | Zpráva | CRC |
|---|---|---|---|---|---|
| MAC **B** | MAC **D** | IP B | IP A | Zpráva | CRC |

*Obrázek 8: Zjednodušená struktura zprávy od A při průchodu mezi směrovači uvnitř sítě (neodpovídá topologii na obrázku 5) a při odchodu ze směrovače, který už je v síti 192.168.1.0/24.*

vání vyšším vrstvám. Základní myšlenka ARP dotazu je zachycena na obrázku 3, odpověď na tento dotaz je zachycena na obrázku 4.

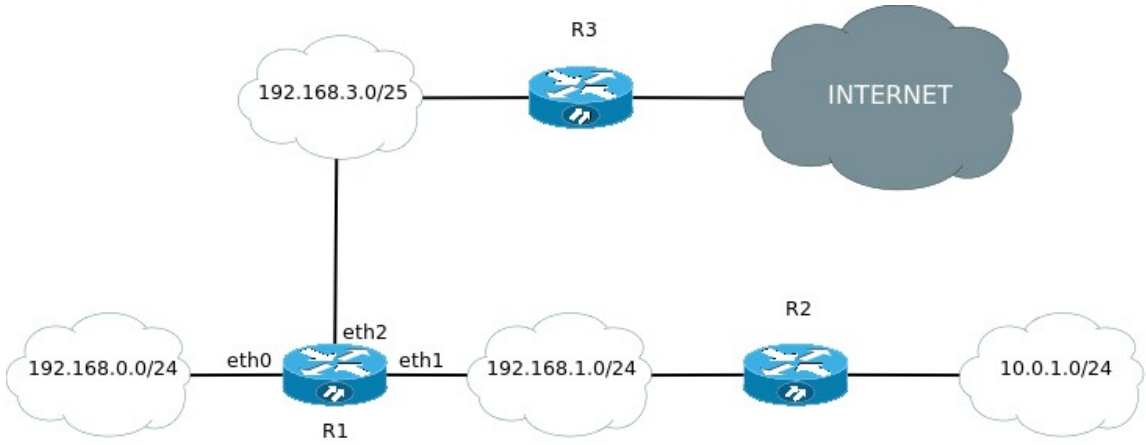
## 3.2 Komunikace mezi sítěmi

V případě, kdy je cílová stanice v jiné síti tedy řádek směrovací tabulky obsahuje nenulovou hodnotu ve sloupci Gateway, není možné s ní komunikovat přímo. I kdybychom znali její MAC adresu a vyplnili ji do rámce, pak tato zpráva nenalezne svého příjemce, protože ji v naší síti nemá kdo přijmout. Proto je nutné využít prostředníka komunikace, v terminologii IP se mu říká *výchozí brána* nebo jenom *brána*, anglicky *gateway*. Brána je taková stanice, která je spojena s více sítěmi a umožňuje všem stanicím v jedné síti komunikaci s ostatními sítěmi. Obecně, každá stanice, která umožňuje komunikaci mezi sítěmi, provádí tedy *směrování* zpráv, se nazývá *směrovač*, anglicky *router* a proto i brána je směrovač.

Jak tedy bude probíhat komunikace mezi stanicí A a B, které jsou v různých sítích? Pro jednoduchost si představme, že naše síť vypadá jako na obrázku 5. Obsahuje tedy jeden směrovač, který je připojen do dvou sítí, každá stanice zná svoji adresu, masku sítě, výchozí bránu a IP adresu protistrany. Stanice A již zjistila, že B je v jiné síti. Jelikož ví, že spojení s ostatními sítěmi jí zajistí brána, musí odeslat zprávu právě k ní. Když pak vytvoří zprávu, jako na obrázku 7, kde jako cílovou adresu 2. vrstvy uvede MAC adresu brány, pak tato zpráva projde sítí 192.168.0.0/24 až k bráně, ta zjistí, že MAC adresa je její, je to tedy zpráva určena pro ni, ale IP adresa už její není. Brána tuto zprávu tedy odešle dál. V tomto případě již rovnou stanici B, ve složitějších případech může zpráva putovat přes několik směrovačů. Vždy se však mění jenom MAC adresy, IP adresy zdroje a cíle zůstávají zachovány po celou cestu komunikace.

## 3.3 Směrování zpráv

Jak ví směrovač, kam má danou zprávu poslat? Odpověď mu dává směrovací tabulka. V ní jsou uloženy informace o přímo připojených sítích, všechny směry, které jsou rozdílné od výchozí brány a výchozí brána. Formát směrovací tabulky pro směrovač R1 z obrázku 9 je zobrazen v tabulce 5.




*Obrázek 9: Síť se složitější topologií.*

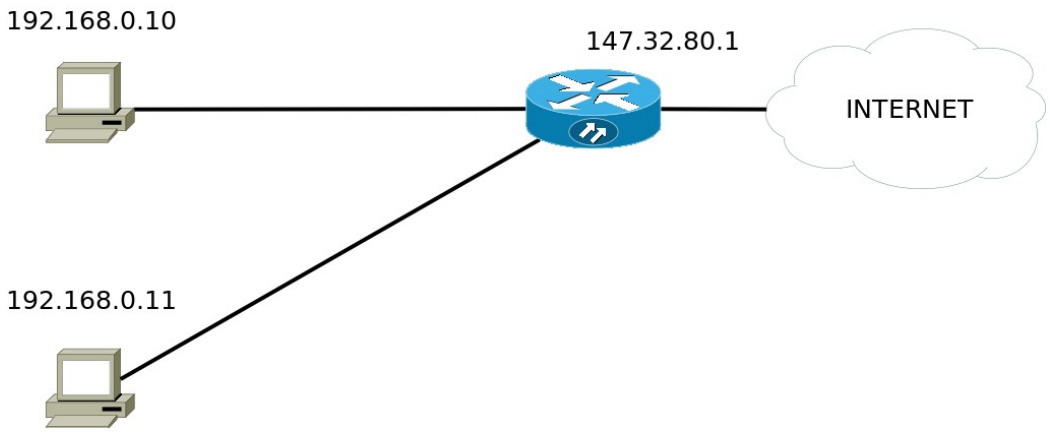
| Destination | Gateway | Mask | Interface |
|---|---|---|---|
| 192.168.0.0 | 0.0.0.0 | 255.255.255.0 | eth0 |
| 192.168.1.0 | 0.0.0.0 | 255.255.255.0 | eth1 |
| 192.168.3.0 | 0.0.0.0 | 255.255.255.128 | eth2 |
| 10.0.1.0 | 192.168.1.15 | 255.255.255.0 | eth1 |
| 0.0.0.0 | 192.168.3.62 | 0.0.0.0 | eth2 |

*Tabulka 5: Směrovací tabulka.*

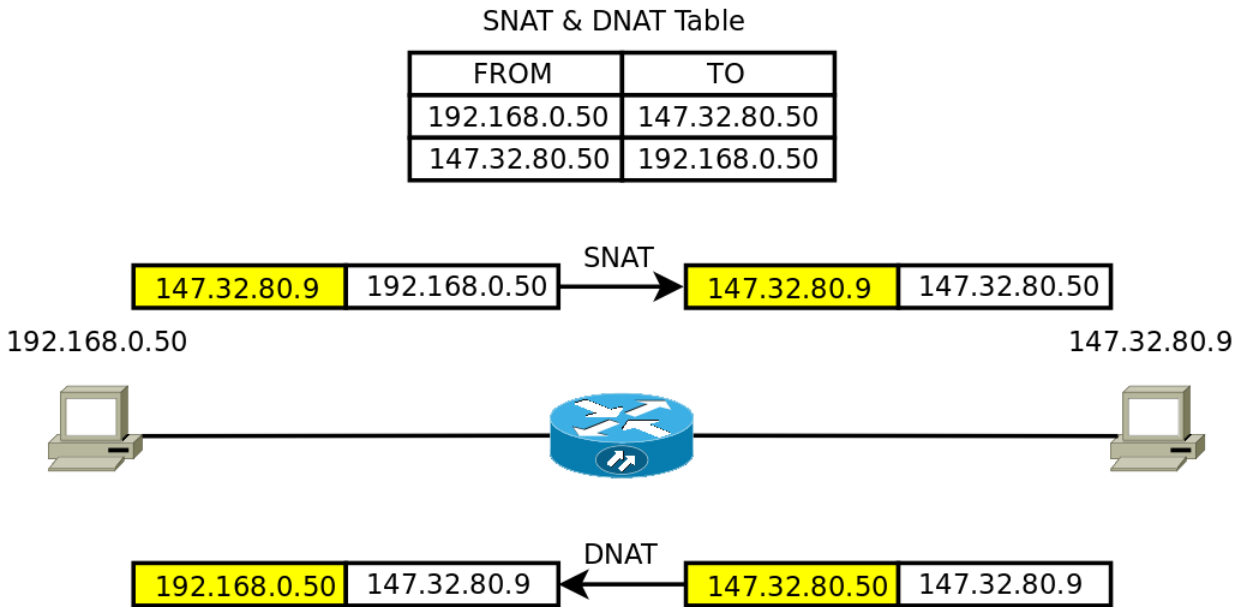
Položka *Destination* je adresa sítě, jejíž maska je uložena v položce *Mask*, směrování do této sítě probíhá přes bránu s IP adresou v položce *Gateway* a v polože *Interface* nalezne směrovač informaci, na které rozhraní se má zpráva odeslat. V tabulce můžete vidět všechny možné záznamy. První tři obsahují informace o přímo připojených sítích (v položce *Gateway* je uložena hodnota 0.0.0.0, tedy tento počítač), další položka obsahuje informaci o síti 10.0.1.0/24, která je umístěna za sítí 192.168.1.0/24 a musí být tedy směrována přes R2. Poslední záznam je výchozí brána. Tento formát zápisu souvisí s algoritmem, kterým je vyhledáván správný směrovací záznam. Ten funguje následovně.

1. Nastav $i na 1, do $dest ulož cílovou adresu zprávy.
2. Vezmi $i-tou položku ze směrovací tabulky a ulož si Masku a Adresu sítě do $mask a $addr.
3. $mezivýsledek = $dest AND $mask {binární operace AND}
4. if ($mezivýsledek == $addr) pošli zprávu podle $i-tého záznamu směrovací tabulky
5. else $i = $i + 1, pokračuj krokem 2.

V celém algoritmu se nevyskytuje žádná informace o tom, že když není vhodné žádné pravidlo, tak je třeba využít výchozí bránu. Tato informace je totiž skryta v posledním záznamu směrovací tabulky. Vezměte si např. adresu 147.32.80.9, která je cílovou adresou zprávy. Při rozhodování, jak s touto zprávou naložit, směrovač projde celou směrovací tabulku. Protože o této síti nemá žádný




*Obrázek 10: Topologie sítě vhodná pro dynamický NAT.*




*Obrázek 11: Zdrojový a cílový překlad adres.*

záznam, dojde až k poslednímu řádku tabulky. Jaké výstupy budou při porovnávání posledního řádku směrovací tabulky jsou ukázány na nasledujících řádcích.

1. $mezivýsledek = 147.32.80.9 AND 0.0.0.0 {provedeme operaci AND s jedním číslem, které má pouze nuly, výsledek jsou tedy opět samé nuly, 0.0.0.0}
2. if ($mezivýsledek {0.0.0.0} == $addr {0.0.0.0} ) pošli zprávu dle pravidla na řádku $i.

Celá „finta“ spočívá v tom, že pokud maskujeme libovolné číslo nulami, výsledek bude vždy nula.

Použití směrovací tabulky u směrovače je zcela očekávané. V textu jsme však již několikrát zmínili, že i stanice mají směrovací tabulky. Jejich struktrura je totožná se směrovacími tabulkami směrovačů, jen většinou obsahují méně řádků. Příkladem budiž tabulka 6, která by mohla být směrovací tabulka libovolné stanice ze sítě 192.168.0.0/24 na obrázku 9.

| **Destination** | **Gateway** | **Mask** | **Interface** |
|---|---|---|---|
| 192.168.0.0 | 0.0.0.0 | 255.255.255.0 | eth0 |
| 0.0.0.0 | 192.168.0.1 | 0.0.0.0 | eth0 |

*Tabulka 6: Směrovací tabulka stanice ze sítě 192.168.0.0/24.*

# 4 Překlad adres

V kapitole 2.7Privátní sítě jsme zmínili, že některé adresy se nesmí vyskytovat na Internetu a každý směrovač musí zprávy s těmito adresami buď zahodit nebo provést překlad adres. *Překlad adres* (Network Address Translation, NAT) je jediná činnost, při které dochází ke změně IP adresy ve zprávě. Rozlišujeme několik technologií, které se obvykle schovávají pod pojmenování NAT.

## 4.1 Statický NAT

*Zdrojový* překlad adres (Source NAT, SNAT) mění adresu odesilatele. *Cílový* překlad adres (Destination NAT, DNAT) mění adresu příjemce. Oba se vzájemně doplňují, pokud je komunikace obousměrná. Jednoduchý příklad ilustruje obrázek 11. Kombinaci SNAT a DNAT se také říká *statický* NAT. U statického NATu vždy mění IP adresy 1:1, proto je nutné, aby pro každou stanici, která má komunikovat s Internetem, byla přidělena jedna veřejná IP adresa.

## 4.2 Překlad portů

Protokolová rodina TCP/IP definuje dva základní protokoly na 4. vrstvě, jedná se o TCP a UDP. Jejich základní funkcí je kromě jiného umožnit komunikovat více aplikacím na jedné stanici současně. K tomuto definuje 4. vrstva tzv. *porty*, tedy čísla, pomocí kterých se jednotivé aplikace odlišují. Každý komunikační kanál je pak rozlišen pomocí pětice IP a port odesilatele a IP a port příjemce a protokolem. Překlad portů tedy probíhá na 4. vrstvě, kdy je přeložen port a IP adresa zůstává zachována.

## 4.3 Dynamický NAT

*Dynamický* NAT kombinuje všechny předchozí druhy překladů adres. Velice často se používá varianta *masquerade*, kterou si nyní popíšeme. V síti na obrázku 10 se nacházejí 2 stanice, jež chtějí komunikovat s Internetem, jejich operátor jim však přidělil jedinou veřejnou IP adresu. Statický NAT tedy nemohou použít. Proto na svém směrovači nastaví dynamický NAT.

Představte si situaci, kdy oba uživatelé budou chtít komunikovat s webovou prezentací portálu www.cvut.cz a jejich požadavky přijdou současně. Směrovač poslouchá komunikaci a ve své tabulce si uloží hodnoty zachycené v tabulce 7.

První řádek tabulky 7 odpovídá prvnímu dotazu, kdy se stanice s IP adresou x.10 zeptala na úvodní stránku. Při dotazu si zvolila jako komunikační port 5600. Než mohla být zpráva odeslána do Internetu, musela být změněna privátní adresa stanice. Adresa odesilatele se tedy nastaví na jedinou veřejnou adresu, která je k dispozici, tedy na 147.32.80.1. Číslo portu může být zachováno, zatím s ním nikdo nekomunikuje. Ještě před koncem první komunikace navázala spojení se stejným serverem stanice s IP adresou x.11. Shodou okolností si zvolila stejný port, ze kterého komunikuje. Překlad zdrojové adresy je stále stejný a jelikož je dvojice 147.32.80.1:5600 již obsazena, dojde v tomto případě i k překladu portu, zvolí se např. nejbližší volný, zde je to port 5601.

Ještě než byla stažena celá úvodní stránka, rozhodla se stanice x.10, že zahájí stažení loga ČVUT. Pro tuto komunikaci si zvolí port 5601 a odešle dotaz na server. Tomuto dotazu odpovídá třetí řádek v tabulce 7. Jelikož je již odchozí port obsazen, dojde opět k překladu portu. Logo stahuje i druhá stanice, ta si však zvolí nekonfliktní port 8500, proto u něj nedochází k překladu. Poslední řádek ilustruje dotaz na google-analytics.com, který je také součástí úvodní stránky ČVUT. První stanice si zvolila komunikační port 5602, který již je na směrovači využit pro jinou komunikaci. V tomto případě však není nutné provádět překlad portu, neboť se jedná o komunikaci s jiným serverem, tedy cílová IP adresa se liší. Toto je dostačující, protože identifikátorem celé komunikace je pětice

hodnot, IP a port cíle a IP a port zdroje. Překladem IP zdroje vždy na stejnou hodnotu pak musí směrovač překládat i porty, aby byl schopen od sebe odlišit rozlišné komunikace různých stanic.

| IP Dest | Port Dest | IP Src | Port Src | IP Trans | Port Trans |
|---|---|---|---|---|---|
| 147.32.3.39 | 80 | 192.168.0.10 | 5600 | 147.32.80.1 | 5600 |
| 147.32.3.39 | 80 | 192.168.0.11 | 5600 | 147.32.80.1 | 5601 |
| 147.32.3.39 | 80 | 192.168.0.10 | 5601 | 147.32.80.1 | 5602 |
| 147.32.3.39 | 80 | 192.168.0.11 | 8500 | 147.32.80.1 | 8500 |
| 173.194.39.100 | 80 | 192.168.0.10 | 5602 | 147.32.80.1 | 5602 |

*Tabulka 7: Překladová tabulka využitá při dynamickém NATu.*

Dynamický NAT má mnoho výhod i nevýhod. Hlavní výhoda spočívá v tom, že za jednu veřejnou IP adresu se mohou schovat tisíce stanic (k dispozici je 16 bitů pro identifikaci portu, jeden směrovač tedy zvládne až 65536 souběžných komunikací, které mohou pocházet až od 65536 stanic). Nejzásadnější nevýhoda NATu je, že komunikaci musí vždy iniciovat stanice za NATem[4], není možnost, jak by mohla komunikaci zahájit stanice s veřejnou IP adresou. Toto úzce souvisí i s možnotí odpovědi. Jakmile stanice za NATem zahájí komunikaci, vytvoří se záznam v překladové tabulce a podle něj může směrovač úspěšně přesměrovat odpověď zpět k původnímu odesilateli. Postup je stejný jako v případě SNATu a DNATu, jen v tomto případě se může překládat i port.

Maškaráda, jak zní český výraz pro masquerade, je dynamický překlad adres, kdy se všechny IP adresy překládají na jedinou adresu. Pokud máme k dispozici více veřejných adres, lze nastavit dynamický NAT tak, aby se využívaly všechny veřejné adresy. Pojem dynamický NAT zahrnuje oba tyto přístupy.

4 Stanice s privátní adresou.

# 5 Reference

1. RFC 791, *INTERNET PROTOCOL*, 9/1981
2. IEEE Std 802-2001. *The Institute of Electrical and Electronics Engineers, Inc. (IEEE)*. 2002-02-07. p. 19. ISBN 0-7381-2941-0
3. RFC 1519, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*, 9/1993
4. RFC 950, *Internet Standard Subnetting Procedure*, 8/1985
5. RFC 1860, *Variable Length Subnet Table For IPv4*, 12/1995
6. RFC 826, *An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses*, 11/1982